TEKNILLINEN KORKEAKOULU

Sähkötekniikan osasto

Olli-Pekka Lintula

ERÄÄN TIEDONSIIRTOVERKON VERKONHALLINTA

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 18. 5. 1990

Työn valvoja Kauko Rahko

TEKNILLINEN KORKEAKOULU DIPLOMITYÖN TIIVISTELMÄ

Tekijä ja työn nimi : Olli-Pekka Lintula

Erään tiedonsiirtoverkon verkonhallinta

Päivämäärä : 18.12. 1989 Sivumäärä : 85

Osasto : Sähkötekniikan osasto Professuuri : Tkl-38 Tietoliikennetekniikka

Työn valvoja : Professori Kauko Rahko

Työn ohjaaja : Professori Kauko Rahko

Kansainvälinen standardointijärjestö ISO on määritellyt avointen järjestelmien viitemallin OSI:n. ISO tulee liittämään tähän viitemalliin myös vastaavan verkonhallinnan mallin. Verkonhallinnan OSI malli jakaa verkonhallinnan toiminnot viiteen ryhmään: Konfiguraation-, vian-, käytön-, turvallisuuden- ja laskutuksenhallinta.

Verkonhallinnan osalta määriteltävä tiedonsiirtoverkko perustuu aikajakoiseen multipleksointitekniikkaan. Verkonhallinnan OSI mallin toiminnot kuvataan ja arvioidaan toimintojen keskinäiset suhteet. Toiminnot määritetään toteutettaviksi kuvatussa tiedonsiirtoverkossa.

Verkonhallinnan toiminnalliset- ja luotettavuusvaatimukset voidaan täyttää parhaiten hajautetusti. Verkonhallinnan toiminnot integroidaan mahdollisimman pitkälle verkon komponentteihin. Verkko pystyy täten suoriutumaan tiedonsiirtotehtävästään itsenäisesti. Keskitetty verkonhallintajärjestelmä suorittaa tehtävät, jotka liittyvät verkon toiminnasta kerätyn tiedon säilytykseen ja jatkojalostukseen. Samoin keskitetty verkonhallinta pystyy tarjoamaan käyttäjäystävällisen käyttöliittymän.

HELSINKI UNIVERSITY OF TECHNOLOGY

ABSTRACT OF THE MASTER'S THESIS

Author and name of the thesis : Olli-Pekka Lintula

The network management of a datacommunications network

Date : 18.12. 1989

Number of pages : 85

Department : Electrical engineering

Professorship : Tkl-38 Telecommunications

Supervisor : Professor Kauko Rahko

Instructor : Professor Kauko Rahko

The international standards organization ISO has undertaken standardization work for network management. ISO has been developing the model for open system interconnection network management in terms of functionality. The network management functions have been divided into five areas: configuration, diagnostics, performance, security and accounting.

A communications network is introduced. The network is based on time division multiplexing technique. The five functional areas of the OSI network management model are introduced and discussed. The network management functions of the example network are discussed and defined.

The requirements for network management reliability and performance are met best in a distributed model. The network management functions are integrated into each of the network elements and the network is thus capable of running independently. The centralized netwokr management system is used for further evaluation of network performance and as an interface to other systems.

HAKUSANAT

Verkonhallinta

Tietoturvallisuus

OSI-viitemalli

Aikajakoinen multiplekseriverkko

ALKULAUSE

Tämä diplomityö on tehty professori Kauko Rahkon johdolla ja ohjaamana, mistä esitän hänelle parhaat kiitokseni.

Työ on tehty Oy Nokia Data Systems Datasiirto tuotekehityksessä. Työn aloitusvaiheessa tuotekehityspäällikkönä ollutta DI Risto Särkilahtea haluan kiittää mahdollisuudesta tämän työn tekemiseen. Mielenkiintoisen tehtävän saamisesta haluan kiittää DI Heikki Santaniemeä. DI Markku Hynnistä haluan kiittää eteenpäinvievästä suhtautumisesta.

Koko Datasiirto-osaston henkilökunta ansaitsee parhaat kiitokset rohkaisevan työympäristön luomisesta. Tutun piristystä ei mikään voi korvata.

Helsingissä 18.12. 1989

Olli-Pekka Lintula
Oskelantie 4aA1
00320 Helsinki

SISÄLLYSLUETTELO

KÄYTETYT MERKINNÄT JA LYHENTEET

TDM	- Time Division Multiplexer Aikajakoinen kanavointilaite
ISO	- International Standards Organization Kansainvälinen standardointijärjestö
OSI	- Open Systems Interconnection Avointen järjestelmien viitemalli
PCM	- Pulse Code Modulation
bps	- bitts per second
CCITT	- The International Telegraph and Telephone Consultative Committee Kansainvälinen neuvoa-antava lennätin-ja puhelinkomitea

1. JOHDANTO

Tietojenkäsittelylaitteiden tehokkuus- ja käytettävyysvaatimukset ovat johtaneet hajautettuihin systeemeihin. Systeemien komponentit ovat kiinteästi toisiinsa kytkettyjä sekä laitteistojen että ohjelmistojen osalta; ne muodostavat verkon. Tällä hetkellä yli puolet yritysten ostamista tietojenkäsittelylaitteista liitetään suoraan johonkin verkkoon. Tiedonsiirto kaikissa sen muodoissa onkin kasvanut tietojenkäsittelyn tahdissa. Tietoliikennemarkkinoiden ennustetaan laajenevan jopa tietojenkäsittelylaitteiden markkinoita nopeammin. /1/

Tiedonsiirron määrän kasvaessa myös laatuvaatimukset ovat kasvaneet. Tiedonsiirto on välttämätöntä tietojenkäsittelyjärjestelmien toiminnalle ja käyttökatkokset saattavat lamauttaa yrityksen toiminnan. Uusimmat sovellutukset vaativat runsaasti kapasiteettia ja nopeita vasteita. Maailmanlaajuiset tietoliikenneyhteydet ovat tuoneet mukanaan kiristyneet tietosuojavaatimukset. Perinteisesti erilaisten järjestelmien; tietojenkäsittely ja tiedonsiirto, on ollut pakko yhdistyä vaatimusten täyttämiseksi. Verkonhallinnan tehtävänä on tarjota menetelmät ja työkalut kasvavan tietoliikenteen laadun ylläpitämiseksi ja parantamiseksi.

Koko atk-alan kasvun aikana tunnusomaista on ollut tekninen monimuotoisuus. Tämä pätee myös tietoliikenneverkkojen kohdalla. Käyttäjien kasvaneet vaatimukset ovat onneksi pysäyttäneet hajaantumisen. Kansainvälinen standardointijärjestö ISO on määritellyt yleisesti hyväksytyn seitsemän-kerroksisen OSI-mallin tiedonsiirtojärjestelmien pohjaksi. Vastaava verkonhallinnan OSI malli tarjoaa standardin eri

tiedonsiirtoverkkojen yhteiselle hallinnalle. Tämä verkonhallinnan malli on useimmilla telehallinnoilla ja toimittajilla perustava lähtökohta uusien järjestelmien määrittelyssä.

Tässä diplomityössä tarkastellaan tietoliikenneverkon verkonhallintaa vastaavan OSI-mallin pohjalta. Tehtäväjaon mukaisia toimintoja arvioidaan sekä yleisesti että toteutettuina aikajakotekniikkaan perustuvassa multiplekseriverkossa. Tavoitteena on integroida verkonhallinta osaksi tiedonsiirtolaitteiden älykkyyttä ja siten automatisoida verkon toimintaa. Erityistä huomiota kiinnitetään tietoturvallisuuden huomioonottamiseen.

2. VERKONHALLINTA JA SEN ASEMA TDM-VERKOSSA

2.1 VERKONHALLINNAN OMINAISUUDET JA VAATIMUKSET

Käsitteelle verkonhallinta ei ole muodostunut selkeää, yksikäsitteistä sisältöä. Verkonhallinnaksi kutsuttujen ominaisuuksien kattama ala tietoliikenneverkon ylläpidosta ja kehityksestä vaihtelee tapauskohtaisesti. Jo rakennettuun verkkoon liitettävän verkonhallintajärjestelmän tehtävät käsitetään yleensä verkon tietoliikenteellisten ominaisuuksien jatkeeksi. Verkonhallintajärjestelmä ei näissä yhteyksissä ole välttämätön varsinaisen tietoliikenteen jatkamiselle ja muutoksille. Toisaalta taas verkonhallinta voidaan nähdä tietoliikennejärjestelmään integroituna osana, jolloin rajanveto ominaisuuksien välillä on vaikeaa eikä järjestelmästä voida erottaa mitään toiminnallisesti itsenäistä osaa vaikuttamatta verkon toimintaan. Tässä diplomityössä verkonhallinnan rooli käsitetään jälkimmäisessä kokonaisvaltaisessa muodossa.

Tietoliikenteen verkonhallinta sai alkunsa keskuskoneeseen tähtimäisesti liitettyjen modeemiyhteyksien valvonnasta. Keskuskoneen edustaprosessoriin liitetyn valvontapäätteen avulla pystyttiin paikallistamaan viallinen yhteys. Muutokset laitteiden toimintaan ja reititykseen vaativat fyysisiä muutoksia. /5/

Verkkojen kasvu ja topologioitten monimuotoisuus on tehnyt tälläisen käytännön mahdottomaksi. Vasta verkon kaikkien komponenttien valvominen ja ohjaaminen keskitetysti yhdestä valvomosta mahdollistaa käytännöllisen toiminnan.

Keskitetty verkonhallinta asettaa verkon komponenteille korkeat vaatimukset. Itse tiedonsiirron lisäksi täytyy niiden kyetä keskustelemaan verkon muiden komponenttien kanssa. Vastaanotettujen viestien perusteella komponentit analysoivat ja muuttavat toimintaansa sekä välittävät viestit muualle verkkoon.

Koska verkon toiminnan jatkuvuus häiriötilanteissa riippuu verkonhallinnasta, asetetaan sen luotettavuusvaatimukset korkealle. Verkonhallinta joka kaatuu verkon mukana, tai jopa ennen sitä, on arvoton. Sen pitää pystyä ainakin valvomaan verkon tilaa kaikissa olosuhteissa vaikka se ei pystyisi turvaamaan tiedonsiirron jatkuvuutta.

Onnistunut verkonhallintajärjestelmä on yhdistelmä keskitystä ja hajautusta; keskitystä koko järjestelmän kontrolloimiseksi, hajautusta resurssien joustavaksi ohjaamiseksi./2/ Käyttäjien tarpeet vaihtelevat työtehtävien mukaan ja verkon tulee muuttua niiden mukana. Tämän vuoksi tiukasti keskitetystä ohjauksesta ollaankin siirtymässä hiukan takaisin, verkon käyttäjät voivat itse ohjata omia resurssejaan. Tässä yhteydessä tulevat esiin suojauskysymykset, kuka saa tehdä ja mitä. Verkon osat, joiden konfiguraatiota käyttäjä pääsee tutkimaan ja muuttamaan, täytyy rajoittaa huolellisesti vain tämän organisaation haltuun.

2.2 VERKONHALLINNAN TEHTÄVÄT

Tehtävät ja niiden jaottelu on tehty OSI:n standardiehdotuksen pohjalta. Tietoliikenneverkon verkonhallinnan tehtävät jaetaan viiteen toimintoon: /6/

- konfiguraationhallinta
- vianhallinta
- käytönhallinta
- tietosuojan hallinta
- laskutuksenhallinta

2.2.1 KONFIGURAATIONHALLINTA

Konfiguraationhallinta toimii verkonhallinnan toimeepanevana osana. Se tarjoaa palvelut muille verkonhallinnan toiminnoille verkon komponenttien toiminnan valvontaan ja ohjaukseen. Hallittavat komponentit voidaan haluttaessa ottaa käyttöön, muuttaa niiden toimintaa ja poistaa käytöstä.

Verkon kulloinenkin topologia sekä laitteiston ja ohjelmistojen rakenne ja tila säilytetään tietokannoissa. Konfiguraationhallinta vastaa näiden tietojen säilytyksestä ja päivityksestä.

2.2.2 VIANHALLINTA

Verkonhallintajärjestelmät saivat alkunsa vikavalvonnasta, koska verkon käytettävyyden kannalta kriittisintä oli vian nopea paikallistaminen. Sittemmin vianhallinnan piiriin on lisätty vian eliminoimisen vaatimat ominaisuudet. /5/

Vian paikallistamiseksi verkonhallinnalla on koko ajan tieto verkon konfiguraatiosta ja aktiivisista yhteyksistä. Ei-aktiivisia osia verkosta testataan jatkuvasti: komponentit suorittavat itsetestit ja siirtotiet mitataan automaattisesti määrätyin väliajoin. Verkonhallinta saa

tiedot sekä aktiivisista että ei-aktiivisista osista ja toimii niiden mukaan. Vian kehittyminen pystytään havaitsemaan mahdollisesti ennen tiedonsiirtoyhteyden katkeamista ja näin ohittamaan vika datasiirron häiriytymättä.

Tärkeä osa vianhallintaa on tilaston pitäminen vikailmoituksista. Verkon ylläpitäjä saa arvokasta tietoa vikaantumistiheyksistä ja pystyy muuttamaan verkon rakennetta sekä rakentamaan varmistukset kriittisten pisteiden mukaan.

2.2.3 KÄYTÖNHALLINTA

Verkon toiminnasta kerätään jatkuvasti tietoa, jotta pystyttäisiin mittamaan verkon toimintaa ja verkon tarjoamien palvelujen laatua. Ylläpidettävän statistiikan avulla tarkkaillaan verkon toimintaa ja suoritetaan vaadittavat muutokset, jotta resurssit olisivat mahdollisimman tehokkaassa käytössä. Käytönhallinta jakautuu seuraaviin toimintoihin: suorituskyvyn valvonta, reitityksen ohjaus, palvelutason mittaus ja erityisryhmien tarpeet. /6/

Suorituskyvyn valvonnan avulla tarkkaillaan laitteiston kykyä suorittaa vaaditut tehtävät. Parametrit valitaan siten, että mittaustulosten avulla saadaan selville laitteiston toiminnan heikkeneminen ennen välityskyvyn keskeytymistä.

Reitityksen ohjauksen avulla huolehditaan varmennusten lisäksi käyttöasteen ja käytettävyyden optimoinnista.

Palvelutasoa mitataan saatavuuden ja yhteyksien laadun avulla. Statistiikkaa kerätään sekä normaalista liikenteestä että suorittamalla testejä yhdessä vianhallinnan kanssa.

Erityisryhmiä palvellaan esille tulevien tarpeiden mukaisesti. Verkonhallinta luodaan mahdollisuuksiltaan joustavaksi, niin että verkon käyttäjien erilaiset tarpeet voidaan huomioida ilman ohjelmistomuutoksia.

2.2.4 TIETOSUOJAN HALLINTA

Verkonhallinnan tehtäviin kuuluu verkon tarjoamien palvelujen tietosuojan tason määrittäminen ja tietosuojapalvelujen tarjoaminen niitä haluavien käytettäviksi. Tietosuojan taso arvioidaan muodostamalla verkon uhkakuva; millä keinoilla tietosuoja on uhattuna ja mitkä ovat riskit. Uhkakuvan perusteella arvioidaan verkon mahdollisuudet havaita ja torjua nämä uhat. /7/

2.2.5 LASKUTUKSEN HALLINTA

Laskutusta varten kerätään tiedot kanavien ja linkkien aktiivisuudesta. Laskutustietojen keräys kuuluu toiminnoiltaan käytönhallinnan piiriin, mutta sen luotettavuus- ja suojausvaatimukset ovat tarkemmat ja korkeammat.

2.3 MULTIPLEKSERIVERKKO

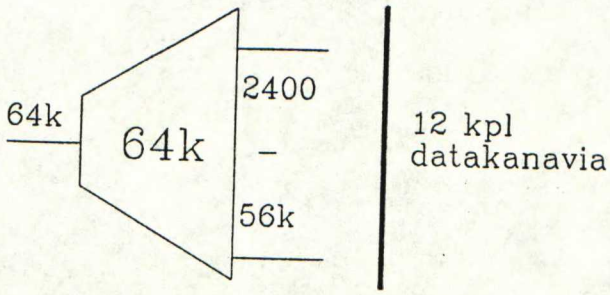
2.3.1 JÄRJESTELMÄKUVAUS

Verkko tarjoaa digitaalisen, piirikytkentäisen tiedonsiirtoyhteyden standardinopeuksille 2400 - 56000 bit/s sekä n*64000 bit/s (n = 1-30). Konfiguraatio- ja topologiavaihtoehdot mahdollistavat vaihtelevankokoiset ja -muotoiset verkot samoja komponetteja käyttämällä, kuten myös kytkentäiset yhteydet ja monipuoliset paikallisverkko-ominaisuudet. Verkonhallinta suoritetaan keskitetysti mikrotietokonepohjaisella järjestelmällä, osa hallinnasta hajautetaan tietoliikenneresurssien vuokraajalle ja asiakkaalle siten että he voivat kontrolloida omia resurssejaan omistä tiloistaan käsin.

2.3.2 VERKON KOMPONENTIT

Aikajakoinen multiplekseri

Multiplekseriverkon peruskomponentti on aikajakoinen multiplekseri (MUX64k), jossa kanavoidaan 2400 - 56000 bit/s kanavat 64000 bit/s (64k) linkille. Linkin datakanavan nopeus on 56 kbit/s, 8 kbit/s käytetään multipleksereiden välisen kontrollitiedon, päätelaitesignaalien tilojen ja kehysrakenteen vaatiman tiedon siirtoon. Multiplekserit yhdistetään digitaalisen verkon tarjoamilla 64 kbit/s yhteyksillä tai lähietäisyyksillä kaapelilla. Multipleksereitten muodostamat solmut liitetään digitaaliseen verkkoon joko suoraan tai solmukeskittimen kautta. Milloin yhteyden pituus tai verkonhallinnan vaatimukset edellyttävät, rakennetaan yhteys linkkimodeemeilla.

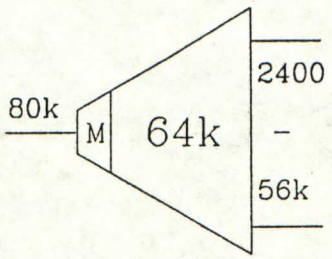


Kuva 1. MUX64k.

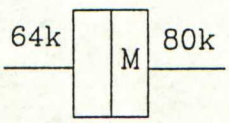
Linkkimodeemit

Tässä esiteltävillä linkkimodeemeilla yhdistetään MUX64k:t sekä erilliset 64k kanavat solmukeskittimeen/ digitaaliseen verkkoon.

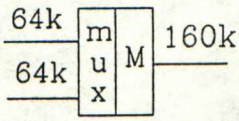
Linkkimodeemit ovat kantataajuusmodeemeja, joiden datakanavan nopeus on 64 kbit/s, tämän lisäksi tarvitaan synkronointikanava 8 kbit/s. Verkonhallinnalle on varattu näiden ulkopuolinen 8 kbit/s kanava, jolloin linjan siirtonopeudeksi saadaan 80 kbit/s. Nopeammalle 160 kbit/s modeemille on multipleksoitu kaksi 64 kbit/s datakanavaa ja niiden vaatimat synkronointi- ja hallintakanavat. Lisäksi n*64k (n=2-30) datakanaville on oma modeeminsa, jossa ei ole erillistä hallintakanavaa.



64 kbps linkkimodeemi yhdistettynä TDM64k:n



80 kbps linkkimodeemi



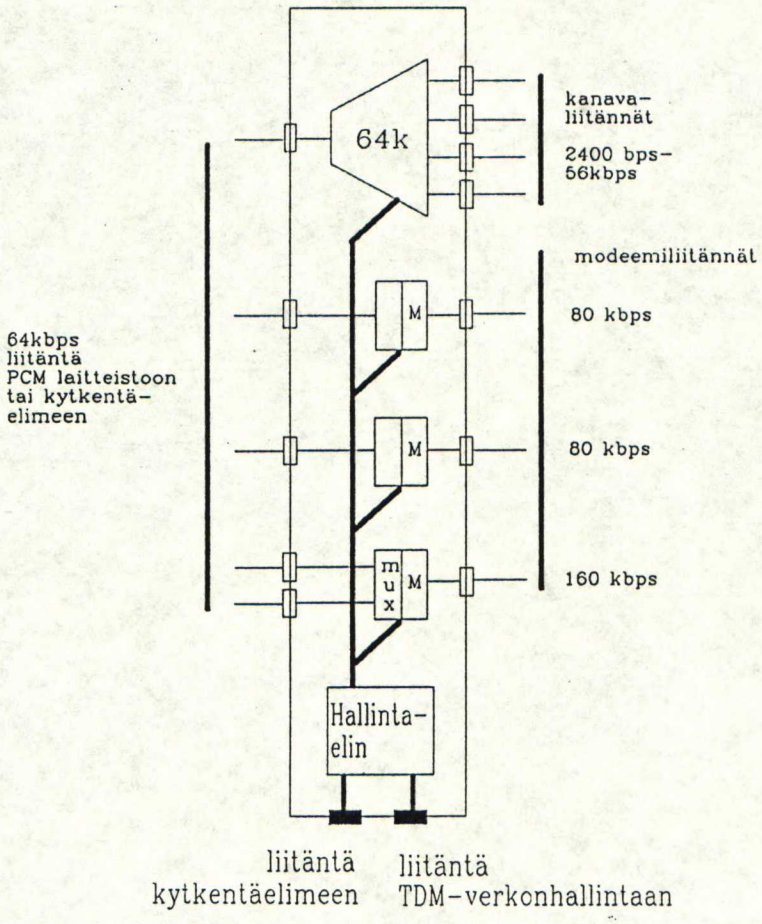
160 kbps linkkimodeemi, joka välittää 2 kpl 64 kbps linkkejä

Kuva 2. Linkkimodeemityypit.

Solmukeskitin

Solmukeskittimen tehtävä on keskittää yksittäisten n*64k (n=1-30) yhteyksien hallinta. Solmukeskitin liittää linkit digitaaliseen verkkoon, mahdollisesti kytkentäelimen kautta. Optionaalisen kytkentäelimen lisäksi solmukeskitin ei puutu päätelaitteiden väliseen tietolii-

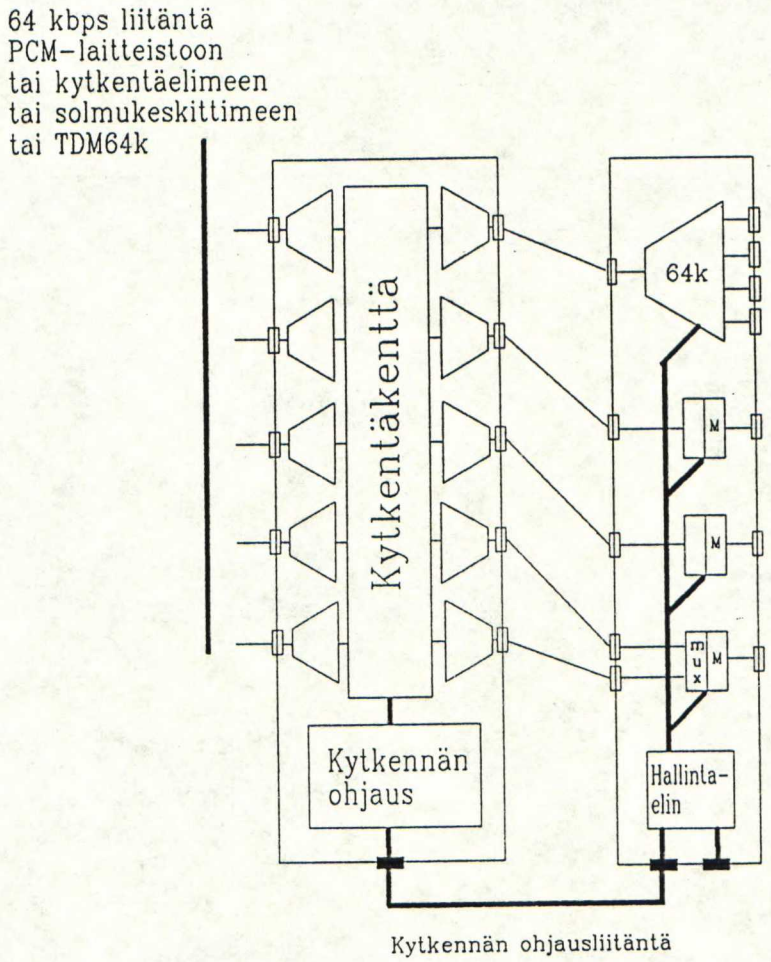
kenteeseen. Tämän liityntäpisteen kautta kytkeydytään TDM-verkon ylemmän tason verkonhallintajärjestelmään ja muihin mahdollisiin verkonhallintajärjestelmiin.



Kuva 3. Solmukeskitin.

Kytkentäelin

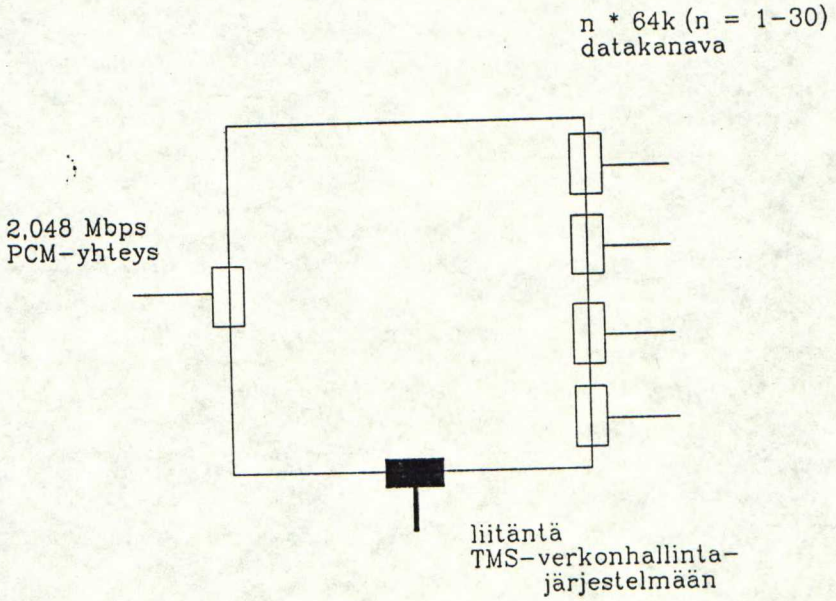
Kytkentäelin sijoitetaan solmukeskittimen ja digitaalisen verkon väliin, sen ytimen muodostaa täysulotteinen kytkentäkenttä. Kytkentäelimessä suoritetaan kanavatason kytkennät, jotka ovat mahdollisia kaikkien kytkentäelimeen liitettävien linkkien ja niiden kanavien välillä. Kanavien tulee olla yhteensopivia.



Kuva 4. Kytkentäelin ja liityntä solmukeskittimeen.

PCM-kanavointilaite

N*64k (n=1-30) yhteyksien vaatimat siirtotiet muodostetaan 2Mbit/s PCM-kanavointilaitteiden (2M PCM) avulla. Ne tarjoavat kytkentäisyyden 64k (linkki) tasolla.

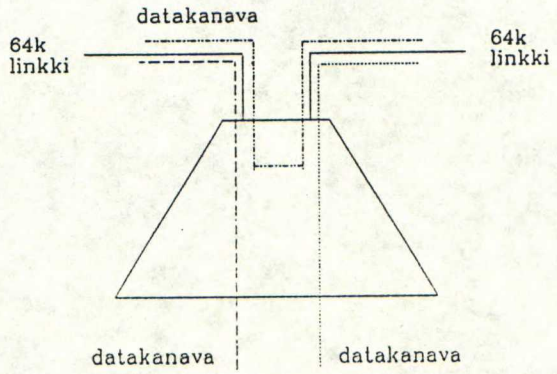


Kuva 5. 2M PCM.

2.3.3 TOPOLOGIAT JA KONFIGURAATIOT

Haaroitus

MUX64k:hon on sisäänrakennettu haaroitusominaisuus. Haaroituksen avulla on mahdollista ohjata kanavat vapaavalintaisesti multiplekserin kahden linkkiyhteyden ja kanavaporttien kesken; linkiltä saapuva kanava ohjataan joko toiselle linkille tai kanavaporttiin (kuva 6.).

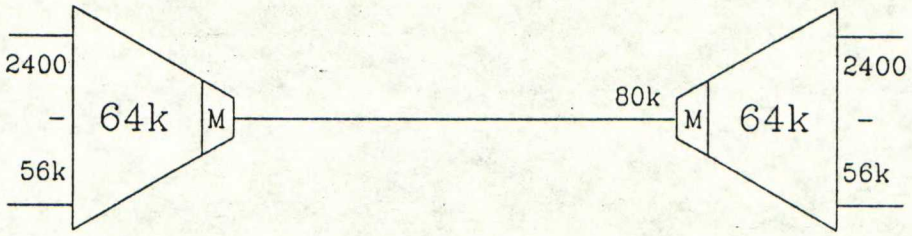


Kuva 6. MUX64k haaroitin.

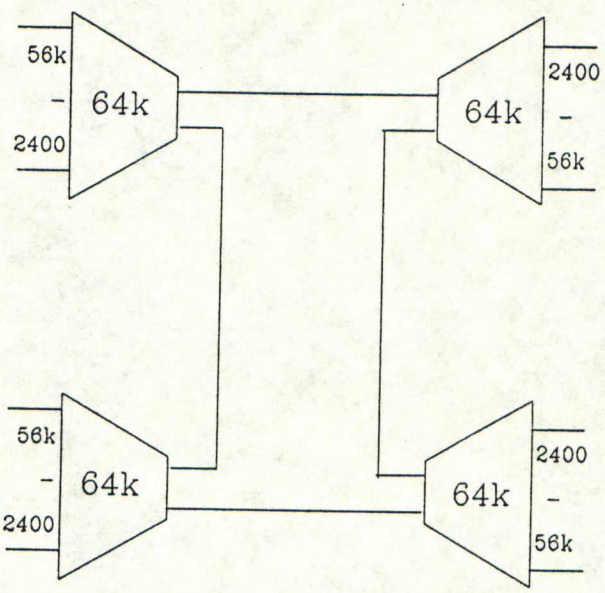
MUX64k-verkko

Päätelaitteiden väliset yhteydet muodostetaan ensisijaisesti MUX64k:sta ja niitä yhdistävistä 64 kbit/s siirtoteistä. Yksinkertaisimillaan on kyseessä kahden pisteen välinen yhteys, kuva 7.

Haaroitusominaisuutta hyväksikäyttäen on mahdollista rakentaa renkaan-muotoinen verkko, renkaan koko (solmujen lukumäärä) määräytyy kanava-nopeuksien ja kanavien määrän perusteella, kuva 8.



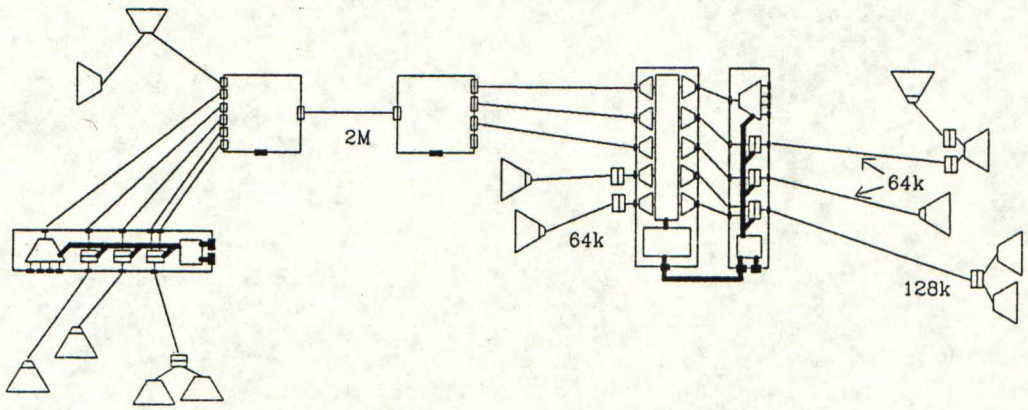
Kuva 7. Kahden pisteen välinen yhteys.



Kuva 8. Rengasverkko.

Laaja verkko

Kuvassa 9. on esitellyistä komponenteista koottu laaja verkko, jonka sisällä ovat kaikki kanavayhteydet mahdollisia. Tämän kaltaisissa verkkoratkaisuissa käytetään hyväksi myös PCM-kanavointilaitteiden kehittyneempiä ominaisuuksia.



Kuva 9. Laaja verkko.

Varatiet

Kaikki siirtotiet voidaan varmentaa käyttämällä varayhteyksiä. Jotta varmistuksesta ei tulisi ainoastaan muodollista, on primääri- ja sekundääriyhteyksillä pyrittävä käyttämään eri tekniikoita, tai huolehtimaan muutoin yhteyksien erilaisesta haavoittuvuudesta.

2.4 VERKONHALLINTA TDM-VERKOSSA

2.4.1 VERKONHALLINNAN OMINAISUUDET

Verkonhallinta kattaa koko TDM-verkon, sen piiriin kuuluvat kaikki verkon komponentit, sikäli kuin niiden ominaisuudet mahdollistavat etäishallinnan. TDM-verkon verkonhallinnan perusta on sen komponenttien, erityisesti MUX64k:n, älykkyys. MUX64k sisältää toiminteet joiden avulla pelkästään niistä rakennettu verkko voi toimia itsenäisenä kokonaisuutena ja keskustella muiden verkonhallintajärjestelmien ja käyttäjien kanssa. Suuria TDM-verkkoja hallitaan keskitetysti solmukeskittimen verkonhallintalaitteiston ja siihen liitettävän verkonhallintatietokoneen avulla.

Verkonhallinta hajautetaan siten että yksittäisten solmujen ja yhteyksien kontrollointi käy päinsä myös tilaajan tiloista ja toimesta. Tällöin resurssien käyttö on joustavaa ja vikatilanteissa toiminta ei ole riippuvainen yhdestä komponentista.

Verkon luotettavuusvaatimuksien vuoksi kaikki komponentit ovat itsenäisiä ja erillisen verkonhallintalaitteiston tehtävänä on toimia lähinnä tiedon jalostajana sekä tarjota monipuolinen käyttäjäliityntä ja liitynnät muihin mahdollisiin verkkoihin ja verkonhallintajärjestelmiin. Verkon toiminta ei ole riippuvainen solmukeskittimen verkonhallintalaitteistosta ja kaikki itse tietoliikenteeseen liittyvät toiminnot sijaitsevat verkon välitin- ja keskitinlaitteissa.

2.4.2 VERKOHALLINTAVERKKO

2.4.2.1 OMINAISUUDET

TDM-verkon hallintatietojen siirrossa pyritään käyttämään hyväksi olemassa olevia yhteyksiä jotta verkon pääfunktio, tiedonsiirto, ei häiriintyisi. Aina se ei ole mahdollista. Käytettäessä ainoastaan valvottavan verkon tarjoamia tiedonsiirtokanavia joudutaan kuitenkin ristiriitaiseen tilanteeseen: vikojen ilmaantuessa katkeavat myös hallintayhteydet, joiden avulla tilanteesta pitäisi toipua. Varayhteydet tuleekin suunnitella alusta pitäen osana verkkoa.

2.4.2.2 VERKON KOMPONENTTIEN VÄLISET YHTEYDET

MUX64K <--> MUX64k

Hallintayhteys multipleksereiden välillä muodostetaan normaalista datakanavasta. Kanavan siirtonopeus riippuu tiedonsiirtotarpeesta; montako multiplekseriä tämä kanava yhdistää hallinnallisesti ja kuinka aktiivisia nämä verkot ovat.

Linkkimodeemi <--> linkkimodeemi

Linkillä olevia modeemeja voidaan hallita kummasta tahansa sitä kontrolloivasta MUX64k:sta käsin. Kaukopään linkkimodeemin kanssa keskustelu tapahtuu kuitenkin modeemien datakanavan kautta, joten se keskeyttää datasiirron.

Solmukeskitin <--> MUX64k (<--> solmukeskitin)

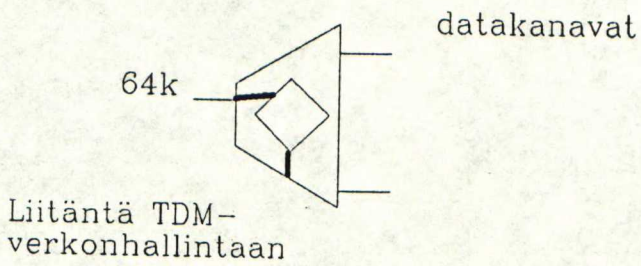
Linkkimodeemien välillä on varsinaisen datakanavan lisäksi 8kbit/s hallintakanava, joka yhdistää solmukeskittimessä sijaitsevan hallintaelimen ja kaukopään multiplekserin. Samalla keinolla yhdistetään haluttaessa kaksi solmukeskitintä.

Solmukeskitin <--> linkkimodeemi

Solmukeskittimessä sijaitseva linkkimodeemi liittyy hallintaelimeen solmukeskittimen sisäisellä väylällä.

TDM-verkko <--> TDM-verkko

Verkonhallintaverkko muodostetaan eri verkkotopologioissa multiplekserissä olevan datahaarukan avulla. Datahaarukkassa on verkonhallintaliitäntä ja sen myötä verkonhallintakanava voidaan joko kytkeä 64k linkille ja/- tai viedä prosessorille analysoitaviksi, kuva 10.

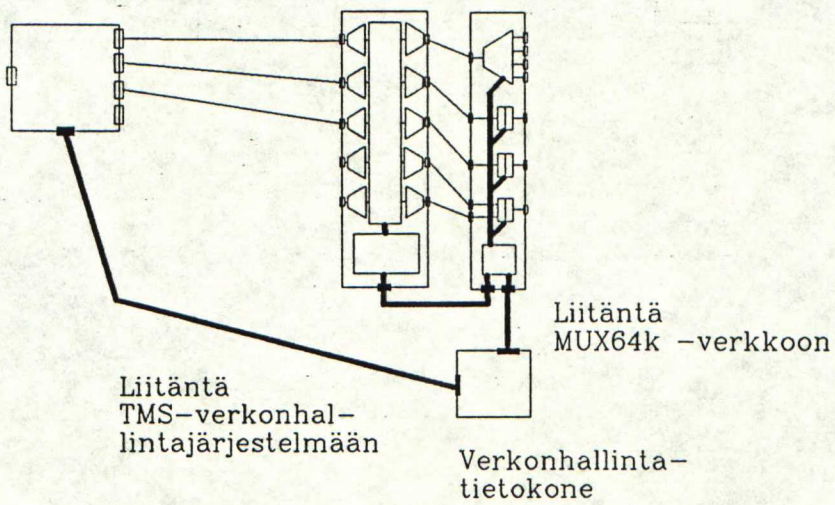


Kuva 10. MUX64k verkonhallintahaarukka.

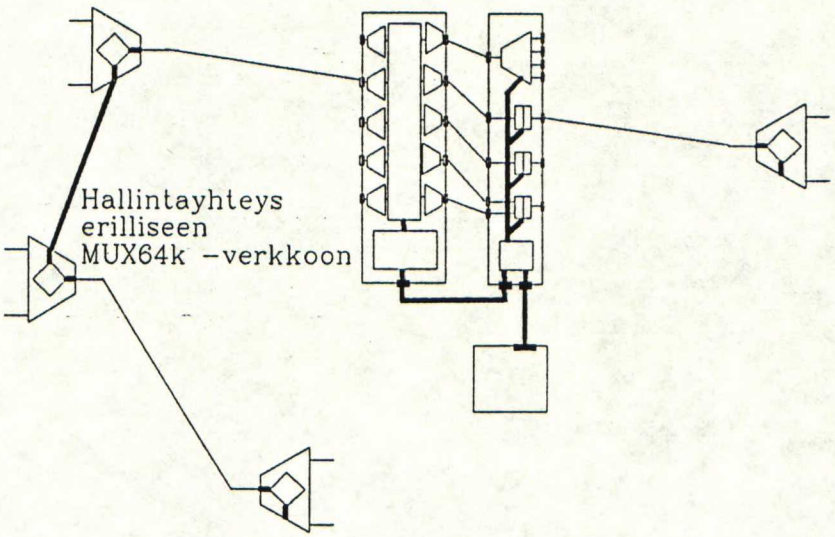
2.4.2.3 VERKONHALLINTAVERKKO

Solmukeskittimen kautta voidaan hallita yhteyksiä ja verkkoja, joilla ei ole omaa solmukeskitintä. Saman verkonhallintatietokoneen kautta on mahdollista kontrolloida useita MUX64k-verkkoja liittämällä nämä hallinnallisesti yhdeksi verkoksi.

Kaikki hallittavissa verkoissa sijaitsevat komponentit liitetään verkonhallintatietokoneeseen. Liityntäpiste verkonhallintatietokoneen ja TDM64k -verkon välillä on solmukeskittimessä sijaitseva hallintaelin. Samaan tietokoneeseen voidaan mahdollisesti keskittää muidenkin tietoliikenneverkkojen verkonhallinta. Liitännät muihin verkkoihin ja/tai verkonhallintajärjestelmiin tehdään TDM64k -verkonhallintatietokoneen avulla.



Kuva 11. Liitäntä muiden tietoliikenneverkkojen verkonhallintaan.



Kuva 12. Verkonhallintaverkko.

2.4.3 KÄYTTÄJÄLIITYNTÄ

Käyttäjä voi liittyä TDM-verkon verkonhallintaan kahta reittiä pitkin: Verkonhallintatietokoneen tai MUX64k:n tarjoaman käyttäjäliitännän kautta. Periaatteessa nämä ovat samanarvoisia; koko verkkoa voi hallita molemmilla tavoilla. Tämä pätee kuitenkin vain verkkoon kohdistuviin toimenpiteisiin; ominaisuuksiltaan ja käyttäjäystävällisyydeltään eri liitännät eivät ole tasa-arvoisia. Verkonhallintatietokone tarjoaa monipuolisemmat tarkkailu- ja analysointikeinot sekä mahdollisuuden monipuoliseen käyttäjäliitäntään, kun taas MUX64k:n käyttäjäliitäntä on toteutukseltaan mahdollisimman tehokas ja yksinkertainen.

3. TDM-VERKON SUOJAUSVAATIMUKSET

3.1 TIETOSUOJA

Tietotekniikan hyödyntämisessä ovat nopeus ja tehokkuus määränneet käyttöönottohetken. Kasvun hallitsemattomuus, joka tuli esiin eri järjestelmiä integroitaessa, näkyy nyt tietosuojan puuttumisena. Usein myös suojautuminen järjestelmän käytettävyyden turvaamiseksi on jäänyt vaille huomiota. Käyttäjien ja lainsäädännön vaatimusten kiristyessä pystytään vain paikkaamaan jätettyjä aukkoja, valitettavasti tämä johtaa usein yhteyksien ja verkkojen purkamiseen. /11/

Koska absoluuttinen suojaus ei ole mahdollista, pyritäänkin suojauksella taloudellisuusnäkökohtien optimointiin; verrataan suojautumisen kustannuksia tunkeutumisen arvioituja kustannuksia ja riskiä vastaan. Toisaalta järjestelmän käytettävyys ei saa kärsiä suojauksista niin, että niitä ruvetaan kiertämään ja suojaustaso itseasiassa laskee. On myös aloja, joissa suojauksen osalta tavoitellaan ehdottomuutta. Tällöin turvaudutaan yleensä perinteisiin menetelmiin: estetään sähköinen tunkeutuminen poistamalla yhteydet ja tiukennetaan kulunvalvontaa, fyysistä suojausta ja henkilöstön luotettavuusvaatimuksia. /8/ /9/

3.1.1 JÄRJESTELMIEN SUOJAUS

Tietosuojan turvaaminen vaatii yhtenäisen lähestymistavan, jossa mikään osa-alue ei saa jäädä huomiotta. Suojausohjelman rakentaminen on systemaattinen menetelmä, joka määrää käytettävät suojausmekanismit tavoitteena olevan suojaustason mukaisesti.

Suojausohjelma aloitetaan kartoittamalla tietojärjestelmään kohdistuvat uhat, ne luokitellaan resurssien (tieto tai tietojärjestelmä): /7/

- tuhoutumiseen
- muuttumiseen
- varkauteen tai katoamiseen
- paljastumiseen
- toiminnan keskeytymiseen

Uhat systeemin suojausta vastaan jaetaan passiivisiin ja aktiivisiin. Passiivinen uhka ei vaikuta tiedonsiirtoon tai systeemin tilaan ja toimintaan. Esim. linjan salakuuntelu on passiivinen uhka. Aktiivinen uhka taasen muuttaa, kopioi, tuhoaa tai lisää tietoa tai vaikuttaa systeemin tilaan ja toimintaan. Esim. reitityskartan muutos on aktiivinen uhka. Uhat voidaan jakaa lisäksi tahallisiin ja tahattomiin.

Muodostettua uhkakuvaa tarkastellaan riskejä vastaan. Arvioidaan miten suuren riskin yksittäiset uhat muodostavat sekä kuinka todennäköisiä ja kalliita ne ovat. Näitä verrataan mahdollisten vahinkojen suuruuteen ja päätetään rationaalisesta suojaustasosta. Tähän suojaustasoon pääsemiseksi on kartoitettava suojausmekanismit todennäköisiksi arvioiduille uhille.

3.1.2 TIETOSUOJA JA ISO

OSI standardiin (ISO 7498, The Basic Reference Model) on lisätty tietosuojaa käsittelevä osa, ISO 7498 Part 2 - Security Architecture. Tässä lisäyksessä kuvataan avoimiin järjestelmiin liittyvät tietosuoja-

palvelut, niiden toteuttamiseen soveltuvat mekanismit sekä näiden mahdolliset sijainnit OSI-viitemallissa. Koska tämä malli esittää ainoastaan tiedonsiirron eri kerrosten palveluiden hierarkian, ei tietosuojankaan määrittely kata koko järjestelmän suojausta. OSI tietosuojamalli antaa puitteet suojausohjelman rakentamiselle mutta sitä täytyy täydentää mallin ulkopuolisilla elementeillä.

Taulukossa 1 on tietosuojapalvelut kussakin OSI-mallin kerroksessa /10/.

Taulukossa 2 on esitetty taulukossa 1 kuvattujen palveluiden toteuttavia mekanismeja. /8/

palvelu	kerros 1	2	3	4	5	6	7
vertaisolion tunnistus			X	X			X
tietolähteen tunnistus			X	X			X
pääsynvalvonta			X	X			X
yhteyden luottamuksellisuus	X	X	X	X			X
yhteydetön luottamuksellisuus		X	X	X			X
valitun kentän luottamuksellisuus							X
liikennevirran luottamuksellisuus	X		X				X
yhteyden eheys toipumismenettelyin				X			X
yhteyden eheys			X	X			X
yhteyden valitun kentän eheys							X
yhteydetön eheys			X	X			X
yhteydetön valitun kentän eheys							X
lähettäjän kiistämättömyys							X
vastaanottajan kiistämättömyys							X

Taulukko 1. Tietosuojapalvelut OSI-mallin kerroksissa

mekanismi							
Notaari							
Reitityksenvalvonta							
Liikenteentäyttö							
Tunnisteidenvaihto							
tiedon Eheys							
Pääsynvalvonta							
Digitaalinen allekirjoitus							
Salaus							
palvelu							
vertaisolion tunnistus	S	D			T		
tietolähteen tunnistus	S	D					
pääsynvalvonta			P				
yhteyden luottamuksellisuus	S					R	
yhteydetön luottamuksellisuus	S					R	
valitun kentän luottamuksellisuus	S						
liikennevirran luottamuksellisuus	S				L	R	
yhteyden eheys toipumismenettelyin	S			E			
yhteyden eheys	S			E			
yhteyden valitun kentän eheys	S			E			
yhteydetön eheys	S	D		E			
yhteydetön valitun kentän eheys	S	D		E			
lähettäjän kiistämättömyys		D		E			N
vastaanottajan kiistämättömyys		D		E			N

Taulukko 2. Tietosuojapalveluiden ja -mekanismien väliset suhteet

OSI-mallin ulkopuolisia turvallisuusmekanismeja ovat mm. luotettujen toimintojen määrittely, väärinkäytöksien havaitseminen ja käsittely sekä turvallisuusloki, johon kirjatut tapahtumat lisäävät kiinnijäämisen riskiä.

3.2 TDM-VERKON SUOJAUSOHJELMA

3.2.1 TAVOITE

TDM-verkon suojausohjelman tavoitteena on turvata datasiirtopalvelujen saatavuus ja tietosuoja sähköisiä uhkia vastaan TDM-verkonhallinnan valvottavissa ja hallittavissa olevien prosessien osalta. Koska estävät toimenpiteet eivät missään olosuhteissa takaa täydellistä suojaa esim. oikeutetun käyttäjäryhmän suorittamia rikkomuksia vastaan, tulee ohjelman taata riittävät kontrollitoiminteet rikkomusten havaitsemiseksi. Tämän vaatimuksen täyttäminen edellyttää, että ko. rikkomus on havaittavissa sähköisin keinoin; esimerkiksi radioyhteyksien salakuuntelua voidaan hankaloittaa salakirjoituksella mutta sitä ei voida havaita.

3.2.2 VERKON UHKAKUVA

Passiiviset uhat:

1. Verkossa siirrettävän datan salakuuntelu

Tiedonsiirtolinjaan kytkeytyen voidaan tutkia välitettävää dataa. Toiminne on teknisesti helppo liitinten yhteydessä ja liityttäessä kaapeleihin sekä radioyhteyksillä, optisten kuitujen kuuntelukaan ei välttämättä vaadi yhteyden katkaisua.

Salakuuntelu on mahdollista myös sähkömagneettisin keinoin kymmenien metrien päästä.

Verkkoon kytketyn pääte- tai välitinlaitteen ominaisuudet saattavat mahdollistaa välitettävän datan tutkimisen esim. toisen kanavan tai kontrolliportin kautta.

2. Verkon hallintatietojen paljastuminen

Pääte- ja välitinlaitteiden sisältämää tietoa verkosta on mahdollista tutkia kytkeytymällä verkon kontrolliprosesseihin.

Aktiiviset uhat:

1. Verkossa siirrettävän datan muuttaminen

Datasiirron häiriintyminen on tavallista häiriöiden vuoksi eikä se saisi estää datasiirron onnistumista. Häiriöt voivat olla sähkömagneettisia kaapeli- ja radioyhteyksillä sekä fyysisiä jälkimmäisellä.

Tahallinen datan muuttaminen käy päinsä kytkeytymällä verkkoon tiedonsiirtolinjan, välitin- tai päätelaitteen kautta. Tunnetuimpia murtautumistapoja ovat naamioituminen sekä kokeilemalla löydettyjen käyttöoikeuksien käyttö.

2. Verkon resurssien käyttö

Tietoliikenneresurssien oikeudeton käyttö on mahdollista kytkeytymällä verkkoon oikeudet omaavaa päätelaitetta simuloiden.

3. Verkon kontrollitietojen ja käytettävyyden manipulointi

Päätelaitteen tiedonsiirto-ominaisuudet ovat alttiita muunteluille usein heikosta suojauksesta johtuen.

Verkon tiedonsiirtolaitteiden asetusten ei-toivottu muuntelu muodostaa suurimman riskin verkon käytettävyydelle ja suojaukselle. Koska laaja verkko sisältää useita käyttäjäryhmiä ja varmennukset vaativat usein valintaisia varateitä on väärinkäytön riski suuri.

Seuraukset

Aktiivisten tai passiivisten uhkien toteutumisen seuraukset riippuvat havaitusta datasta ja kytkeytymistavasta. Useinkaan välitettävän datan paljastuminen tai datasiirron väliaikainen häiriintyminen ei sinällään ole kovin vaarallista tai merkittävää. Verkon kannalta vaarallisempaa on käyttöoikeuksien paljastumisen kautta leviävä mahdollisuus kytkeytyä verkkoon tai verkonhallintajärjestelmään.

3.2.3 TOTEUTETTAVAT TIETOSUOJAPALVELUT JA -MEKANISMIT

TDM-verkonhallinta muodostaa itsessään tietoliikenneverkon, joka käsittää kaikki OSI-mallin seitsemän kerrosta. Tämä verkonhallintaverkko käyttää osittain hyväkseen TDM-verkon tarjoamia OSI-mallin kolmen alimman kerroksen palveluita.

Tietosuojapalvelut ja ne toteuttavat mekanismit jaetaan sen mukaan kuuluuko suojattava toiminto TDM-verkon tarjoamiin tiedonsiirtopalveluihin vai TDM-verkonhallinnan piiriin. Koska TDM-verkonhallinta käyttää myös TDM-verkon ulkopuolisia tiedonsiirtopalveluja, täytyy näiden suojaustasosta varmistua erikseen. Vaadittava suojaustaso ei saa alittaa TDM-verkolta vaadittavaa tasoa miltään osin.

3.2.4 TDM-VERKON TIETOSUOJAPALVELUT JA -MEKANISMIT

Luotetut toiminnot:

TDM-verkonhallinnan hallinnassa olevien tietoliikennelaitteiden ohjelmistojen ja laitteistojen oletetaan olevan puhtaita tietosuojaa heikentävistä piirteistä, kuten luukuista.

Torjuttavat uhat:

Verkon **tiedonsiirtopalvelujen oikeudeton käyttö** tulee estää. Vaatimus pitää sisällään sekä päätelaitteiden kytkeytymisen verkkoon että TDM:n keskinäisen kytkeytymisen.

Päätelaitteita kontrolloidaan suojaamalla määrätyt portit molemminsuuntaisesti; kytkeytyminen sekä päätelaiteliitännän että kanavan kautta voidaan estää. Suojauspalveluna käytetään pääsynvalvontaa. Kontrolloitavaksi määrättyä porttia suojataan käyttäjätunnuksen ja salasanan, ajankohtaan liittyvien rajoitusten ja reitin avulla. Kaikkia mekanismeja voidaan käyttää joko erikseen tai haluttuna kombinaationa. Esim. liittyminen modeemiyhteyden kautta keskustietokoneeseen voi olla käyttäjätunnuksen ja salasanan suojaama työaikana ja estetty työajan ulkopuolella.

Suojatuissa porteissa rajoitetaan peräkkäisten epäonnistuneiden yritysten lukumäärä kaikissa tapauksissa kuuteen kertaan, jonka jälkeen portti lukitaan myöhemmältä käytöltä. Portin vapautus voidaan suorittaa ainoastaan verkonhallintatoimintojen avulla manuaalisesti ja/tai aikavalvonnan kautta.

Mikäli resurssien käyttö on estetty reitin tai ajankohdan perusteella, ei yhteydenottoyrityksen yhteydessä saa käyttäjälle antaa minkäänlaista tervehdystä tai ilmoittaa syytä yrityksen epäonnistumiseen. Käyttäjää avustavien toimintojen toteutus yhteydenottoa varten on kielletty.

TDM:n liittyminen verkkoon suojataan aina kahdenvälisellä vertaisolion tunnistuksella ja pääsynvalvonnalla. TDM:t tunnistavat toisensa tunnisteidenvaihdon avulla. Kussakin TDM:ssa on pääsynvalvontatietokanta, johon ym. tunnisteet on sijoitettu. Yhteydenmuodostus voidaan evätä tunnisteille myönnettyjen rajoitusten perusteella.

Verkon välittämän **datan salakuuntelu ja datasiirron häirintä** tulee pyrkiä estämään salakuuntelulle kriittisin osin käyttämällä yhteyden luottamuksellisuuden mekanismeja. Salakuuntelulle altiit tietoliikenneyhteydet, esim. radioyhteydet, suojataan salakirjoituksella ja varmistetaan toista tiedonsiirtotekniikkaa käyttäen. Reititysmekanismien avulla kierretään ongelmapaikat, tässä voidaan käyttää joko automaattista tai manuaalista reititystä. Esim. aamukasteen tiedetään häiritsevän radiolinkkiyhteyksien käyttöä.

Rekisteröitävät tapahtumat:

Kaikista kontrolloitujen porttien kautta tehdyistä yhteydenotoista talletetaan ajankohta ja tieto mistä portista yhteydenotto tehtiin. Nämä ja tieto mahdollisista epäonnistuneista yhteydenottoyrityksistä samalla käyttäjätunnuksella ilmoitetaan käyttäjälle hänen kytkeytyessään seuraavan kerran. Epäonnistuneista yhteydenottoyrityksistä talletetaan lisäksi reitti ja epäonnistumisen syy.

Häiriöiden vuoksi tehtävästä reititysmuutoksesta talletetaan verkon osa, johon häiriö kohdistui tai oletettiin kohdistuvan, häiriön laatu, havainnon ajankohta, reititysmuutoksen ajankohta, uusi reitti ja muutoksen suorittaja: automaattinen/manuaalinen (kuka).

3.2.5 TDM-VERKONHALLINNAN TIETOSUOJAPALVELUT JA -MEKANISMIT

Luotetut toiminnot:

TDM-verkonhallinnassa ei ole tietosuojaa heikentäviä piirteitä.

Torjuttavat uhat:

TDM-verkonhallinnan salakuuntelu pyritään estämään samoin mekanismein kuin verkon välittämän datan kohdalla.

TDM-verkonhallinnan toimintojen oikeudeton käyttö tulee estää. Käyttäjäliitynnässä oikeudet tarkistetaan pääsynvalvonnan avulla, verkon sisällä vaaditaan solmujen välisten viestien yhteydessä tietolähteen tunnistus. Pääsynvalvonnassa käytetään käyttäjätunnusta ja salasanaa. Tietolähteen tunnistus suoritetaan kullekin solmulle annetun salasanan ja aika-leima-tekniikan avulla.

Käyttäjäliitynnässä rajoitetaan peräkkäisten epäonnistuneitten yhteydenottoyritysten lukumäärä kuuteen, jonka jälkeen ko. käyttäjätunnukselta evätään yhteydenotot. Kyseessä ollut portti lukitaan, vapautus tapahtuu aikavalvonnan tai manuaalisen vapautuksen kautta.

Mikäli verkon solmujen välisessä liikenteessä havaitaan tietolähteen tunnistuksen vajavaisuuksia, esim. aika-leiman suhteen, otetaan lähettäneen solmun verkonhallintaan yhteys varatietä. Mikäli se ei ole mahdollista keskeytetään liikenne ko. solmun kanssa ja lähetetään vastaava viesti muille verkon solmuille.

Verkonhallinnan oikeudet jaetaan käyttäjille käyttäjäryhmittäin, jolloin resurssien ohjaus voidaan suorittaa tilaajan toimesta. Käyttäjä kuuluu eri käyttäjäryhmiin riippuen kytkeytymisajankohdasta ja -reitistä. Kullekin käyttäjäryhmälle määritellään toimintoryhmä ja osaverkko, jossa toiminnot ovat voimassa.

TDM-verkko voidaan jakaa käyttäjäryhmien hallitsemiin osaverkkoihin seuraavasti (hallittavat prosessit on voitu toteuttaa missä tahansa verkon komponentissa):

a) portti ja siihen mahdollisesti kytketyt tiedonsiirtolaitteet
b) yhteys TDM-porttien välillä
c) yhteyskimppu
d) TDM-verkko

Toimintojen suojausvaatimukset eritellään myöhemmin, käyttäjäryhmät jaetaan niiden mukaisesti neljään luokkaan:

a) oikeus monitoroida konfiguraatiota ja testi- sekä käytönvalvontamittauksia

b) kuten a) ja oikeus suorittaa konfiguraatiomuutoksia ja testejä

c) kaikki oikeudet

d) erityisryhmät, kuten laskutuksen seuranta

Rekisteröitävät tapahtumat:

Kytkeytymisestä verkonhallintajärjestelmään pidetään kirjaa; käyttäjä, kytkeytymisajankohta ja -reitti. Nämä tiedot ja onko hänen käyttäjätunnuksellaan tehty epäonnistuneita kytkeytymisyrityksiä ilmoitetaan ko. käyttäjälle hänen kytkeytyessään seuraavan kerran.

Reititysmuutokset kirjataan: uusi reitti, ajankohta, muutoksen suorittaja (automaattinen/manuaalinen (kuka)) ja mahdollisesti syy.

Muut tietosuojapalvelut ja -vaatimukset:

Turvallisuuslokia pidetään rekisteröitäviksi määrätyistä tapahtumista. Lokiin kirjattuja tapahtumia ei voi sieltä poistaa ja tietojen pitää säilyä vähintään kolme vuorokautta. Kaikki reititysmuutokset sekä tietosuojan murtoyritykset tulostetaan reaaliajassa keskusvalvomon tulostimelle.

Salasanojen pituus pitää olla vähintään kuusi merkkiä. Salasanat talletetaan verkonhallintaan käyttäen yksisuuntaista salakirjoitusta.

Verkonhallintaan kytketyissä järjestelmissä ei saa suorittaa ohjelmankehitystä, asennettuja ohjelmia ei saa tutkia, kopioida eikä muuttaa. Ohjelmien lisäys ja vaihto vaativat erityisoikeudet, jotka myönnetään rajattuina kussakin tapauksessa erikseen.

Valintaiset yhteydet suojataan vastasoittolaitteella, jonka lähteviin linjoihin on yleisessä keskuksessa määritetty soitonesto.

4. KÄYTÖNHALLINTA

4.1 TEHTÄVÄ

Käytönhallinta tarjoaa toiminnot, joiden avulla huolehditaan TDM-verkon optimaalisesta tiedonsiirtokyvystä sekä lyhyellä että pitkällä tähtäyksellä. Lisäksi se tarjoaa toiminnot erityisryhmien tarpeisiin. Käytönhallinta jaetaan seuraaviin osiin: toiminnan valvonta, palvelutason valvonta ja reitityksen ohjaus. TDM-verkossa on laskutuksen tarve pieni, joten kaikki siihen liittyvät toiminnot luetaan käytönhallinnan piiriin. Laskutuksesta huolehtivat elimet lasketaan erityisryhmäksi.

4.2 TOIMINNAN VALVONTA

4.2.1 TAVOITTEET

Toiminnan valvonnan rooli automaattisessa verkonhallinnassa on korjata akuutit tiedonsiirron resurssi- ja laatuongelmat sekä yhdessä vianhallinnan ja palvelutason valvonnan kanssa pyrkiä ennakoivaan käyttökatkosten torjuntaan. Verkon kunnosta ja kehityksestä vastaavalle henkilökunnalle tarjotaan tarvittavat tiedot varauduttaessa käytön mukanaan tuomiin vaatimuksiin sekä verkon tiedonsiirto- että hallintaominaisuuksien osalta.

Verkon tilaa ja toimintaa mitataan jatkuvasti ja näistä mittauksista ylläpidetään statistiikkaa. Valittavien parametrien avulla mitataan tietoliikenteen määrää ja arvioidaan verkon konfiguraation kykyä vastata kapasiteettitarpeisiin. Mittausten tulokset ovat luonteeltaan kvan-

titatiivisia, palvelutason määrittelyn taasen kvalitatiivisia. Molempia näkökohtia tarvitaan muutettaessa verkon konfiguraatiota vastaamaan tiedonsiirtovaateita sekä lyhyellä että pitkällä tähtäimellä.

4.2.2 YLLÄPIDETTÄVÄ STATISTIIKKA

4.2.2.1 Tarvekartoitus

Statistiikan keräämien tietojen tarvitsijat ovat automaattinen ja manuaalinen verkonhallinta. Niiden tarpeet poikkeavat toisistaan tiedon luonteen ja jalostusasteen mukaan. Automaattinen verkonhallinta pyrkii tosiaikaiseen toiminnan optimointiin ja korjaukseen. Se vaatii jalostettua tietoa, josta voidaan suoraan osoittaa muutoksia vaativat laitteet ja toiminteet. Manuaaliset verkkoon kohdistuvat toimenpiteet taasen tarvitsevat yksityiskohtaisempaa tietoa, jota on mahdollista tutkia eri näkökulmista.

4.2.2.2 Automaattisen verkonhallinnan vaatimukset

Verkonhallinnan itsenäisesti tekemät toimenpiteet koskevat: Resurssien tehotonta käyttöä, kapasiteetin puutetta ja ennakoivaa vikojen torjuntaa. Viimeinen kohta vaatii kvalitatiivista tietoa, jonka kerääminen kuuluu palvelutason määrityksen piiriin. Resurssien käytön optimoinnissa luonnollinen mittari on käyttöaste.

4.2.2.3 Manuaalisten muutosten vaatimukset

Tietoliikenneverkkojen mitoitus ei kuulu tämän työn piiriin, mutta määriteltävän järjestelmän tulee taata tarkoituksenmukaiset tiedot myös mitoituksen tarpeisiin. Ei-automaattisesti tehtävät arvioinnit ja muutokset käyttävät pohjanaan samoja kriteerejä kuin automaattinen verkonhallinta. Lisävaatimuksena on pidempi aikajänne.

4.2.2.4 Verkonhallinnan kehittäminen

Koska verkonhallintaverkko ei aina vastaa tiedonsiirtoverkon topologiaa, täytyy sen toimintaa tarkkailla erillisenä. Tärkein ominaisuus on yhteyksien saatavuus, sitä mitataan verkonhallintaan osallistuvien komponenttien aikaestolla. Hyvä mittari kuormitukselle on käskyjen vasteaika. Varmuutta mitataan käskyjen uusimistarpeella.

4.2.2.5 Mittaukset

TDM-verkosta kerättavät tiedot jaetaan kahteen ryhmään: tietoliikenne ja verkon kontrollitoiminteet.

a) Tietoliikenne

Tietoliikenne-mittauksilla pyritään saamaan selville verkon kuormitus ajan ja paikan funktiona. Tätä varten suoritetaan seuraavat mittaukset:

1. Porttikohtaiset

- yhteydenottoyritysten lukumäärä
- käyttöaste

2. Linkkikohtaiset

- yhteydenottoyritysten lukumäärä
- käyttöaste

3. Kanavakohtaiset

- yhteydenottoyritysten lukumäärä
- käyttöaste

Käyttöastetta koskevat tiedot pitää kaikilta osin päivittää 1s välein. Automaattisen verkon valvonnan tarpeisiin suoritetaan käyttöasteen mittauksille jaksotus viidentoista minuutin osiin kalenterijaolla. Tarkkuusvaatimus on 0,1% . Nämä tiedot säilytetään kalenteriviikon ajan. Kaikki mittaustulokset säilytetään yhden kalenterivuorokauden ajan.

b) Verkon kontrollitoiminteet

Nämä mittaukset auttavat arvioimaan tietoliikenteen ohjauksen tehokkuutta ja verkonhallinnan toimintaa.

1. Komponenttikohtaisesti

- aikaesto
    - keskiarvo ja varianssi 15 min jaksoissa
    - kumulatiivinen aikaesto
    - tarkkuus sekuntti

- vasteaika
    - keskiarvo ja varianssi 15 min jaksoissa
    - tarkkuus 0,1 s
- käskyjen toistotarve

Kaikkien tietojen säilytysaika vähintään vuorokausi.

4.2.2.6 Tietojen analysointi ja yhteistyö verkonhallinnan muiden toimintojen kanssa

TDM-verkon toiminnan turvaamiseksi ja edistämiseksi suoritettavat toimenpiteet riippuvat kyseesssä olevasta konfiguraatiosta; mihin se kykenee ja mikä on tarkoituksenmukaista. Kaikkien muutosten tulee lähteä tarpeesta ja kehittää verkkoa kokonaisuutena. Kehityskriteerejä ovat koko verkon:

a) tietosuoja
b) käytettävissä oleva kapasiteetti
c) palvelutaso
d) hallittavuus
e) suoranaiset kustannukset
f) välilliset kustannukset

Kohta f) kuuluu manuaalisen verkonhallinnan piiriin eikä sitä vaadita huomioonotettavaksi selvitettäessä akuutteja kapasiteettiongelmia. Muutoin kriteerit on esitetty prioriteettijärjestyksessä.

Toiminnan valvonta toimii kiinteässä yhteistyössä palvelutason valvonnan kanssa. Muutokset tehdään joko kapasiteetin loppuessa tai palvelutason heiketessä alle hyväksyttävän tason. Tietosuojan rooli on monilmeinen; sen avulla voidaan määrätä käytettävät reitit, priorisoida yhteydet ja estää jonkin reitin käyttö. Muut kriteerit eivät aikaansaa muutosta, ainoastaan priorisoivat eri reititysvaihtoehdot.

Päätöksenteko tehtävästä muutoksesta perustuu sekä hetkelliseen että historiatietoon. Toiminnan valvonnan ja palvelustason valvonnan pitämistä tilastoista voidaan arvioida reittien nykyinen taso ja sen vaihtelut ajan mittaan.

4.3 PALVELUTASON VALVONTA

4.3.1 TAVOITTEET

Tavoitteena on valita mittarit ja määritellä niiden käyttö, jotta voidaan arvioida TDM-verkon ylemmille verkkokerroksille tarjoamien palvelujen laatu. Verkon sisäisiin toimintoihin tai niiden laatuun ei oteta kantaa, ainoastaan ulospäin näkyviin seikkoihin. Palvelutasomittauksia käytetään muitten käytönhallinnan toimintojen apuna, eikä suoraan niiden perusteella suoriteta automaattisia muutoksia verkkoon.

Palvelutason mittausten pohjana ovat CCITT:n suositukset X.130, X.131, X.140 ja X.213. Niissä määritellään yleiset palvelutason parametrit, yhteydet OSI standardeihin sekä mittaukset piirikytkentäisissä verkoissa.

4.3.2 PALVELUTASON MITTAUS

4.3.2.1 Mitattavat suureet

Palvelutasoa mitataan kahdesta näkökulmasta: Tiedonsiirtoverkon suorituskykyvyn mittaukset ja ei-suorituskykyyn liittyvät suureet. Suorituskyvyn mittaukset kertovat tiedonsiirtoverkon kyvyn suorittaa vaaditut toimenpiteet, ne jaetaan kolmeen osaan: Yhteyden muodostus, yhteyden laatu, yhteyden purku. Ei-suorituskykyyn liittyvät suureet kertovat muut ulospäin näkyvät ominaisuudet.

Kaikilta suorituskyvyn osa-alueilta valitaan vähintään yksi laatuparametri. Muista ominaisuuksista otetaan huomioon erityisesti TDM-verkkoa ja sen tarjoamien palvelujen tasoa kuvaavat. Näistä kaikista mittauksista suoritetaan yhteenveto, jonka perusteella muut verkonhallinnan toiminnot voivat suorittaa tarvittavat toimenpiteet.

4.3.2.2 Suorituskyvyn mittaus

a) yhteyden muodostus

Palvelutaso piirikytkentäisissä verkoissa, kuten TDM-verkko, määräytyy yhteyden muodostamisen osalta kahdesta parametrista /12/: Yhteyden muodostumisen kesto (saantiviive) ja saannin esto.

Saannin estotodennäköisyys lasketaan valittuna ajanjaksona kutsuestona; muodostumatta jääneiden saantiyritysten suhde kaikkiin saantiyrityksiin.

Lisäominaisuutena otetaan mukaan kertaluenteinen, ennalta määrättävissä oleva yhteydenmuodostusviiveen mittaus, mutta jatkuvaa tilastointia ei vaadita suoritettavaksi.

b) yhteyden laatu

Yhteyden laatu ilmaistaan yhteydellä mitatulla bittivirhesuhteella /13/. Mittaustulokset saadaan joko automaattisen verkonhallinnan suorittamista tai manuaalisista mittauksista.

c) yhteyden purku

Yhteyden purkamisen osalta käytetään palvelutason mittarina sen kestoaikaa (purkuviive) /12/.

4.3.2.3 Ei-suorituskykyyn liittyvät suureet

TDM-verkossa vaikuttavat tarjottavien tiedonsiirtopalvelujen laatuun: Yhteyden tietosuoja ja yhteyden prioriteetti. Molemmat ovat muissa yhteyksissä yksikäsitteisesti määrättyjä.

4.3.2.4 Tilastojen keräys ja säilytys

Tilastollisia, mitattuja tuloksia yhteyden laadusta kerätään jatkuvasti vähintään kahdessa ko. yhteyden muodostavassa TDM-verkon komponentissa. Mittaustuloksia säilytetään vähintään yksi viikko tai kunnes ne on siirretty jatkokäsittelyä varten.

4.3.2.5 Mittausten tulkinta ja yhteenveto

Suorituskykyyn liittyvien mittausten tulokset ilmaistaan kalenteritunnin, -vuorokauden ja -viikon jaksoina. Bittivirhesuhteen osalta ko. ajanjaksoilta ilmaistaan keskiarvo ja huippuarvo.

Kaikkien palvelutason parametrien arvot tulkitaan s.e. palvelutaso on joko tyydyttävää tai ei-tyydyttävää. Kiinteille yhteyksille ja valintaisille porteille lasketaan käytettävyys; sen ajan suhde kokonaistarkasteluaikaan, jolloin tyydyttävä palvelu on saatavilla. Minkä tahansa palvelutason parametrin raja-arvon ylitys johtaa palvelutason laskemisen ei-tyydyttäväksi. Käytettävyys ilmaistaan samoina ajanjaksoina kuin eri mittausten tulokset.

Suorituskyvyn parametrien raja-arvot:

parametri	raja-arvo	
saantiviive	1900ms	/14/
saannin esto	5%	/15/
bittivirhesuhde	10^{-7}	/16/
purkuviive	900ms	/17/

Ei-suorituskykyyn liittyvistä parametreistä tietosuojan heikkeneminen saataa pudottaa palvelutason ei-tyydyttäväksi. Tieto tietosuojan ratkaisevasta heikkenemisestä saadaan tosiaikaisesti sitä tarkkailevalta elimeltä.

4.3.2.6 Yhteistyö verkonhallinnan muiden toimintojen kanssa

Palvelutason valvonta tietoa jakelevana elimenä, ja sille asetettavia vaatimuksia voidaan muuttaa muiden toimintojen vaatimusten muuttuessa.

4.4 REITITYKSEN OHJAUS

4.4.1 TAVOITTEET

Reitityksen ohjaukselle asetetaan kaksi vaatimusta: toimia keskitettynä elimenä, joka kontrolloi automaattista verkonhallintaa ja sen toimintojen ehdotuksia sekä tarjota käyttäjälle hänen tiedonsiirtoaan helpottavia piirteitä.

Eritoten laajoissa verkoissa on kerättävän ja analysoitavan tiedon määrä suuri ja tarvitaan kokoava elin, joka pystyy priorisoimaan eri toimintojen vaateet. Reitityksen ohjaus toimii hyväksyvänä ja päättävänä elimenä verkon konfiguraatioon kohdistuvissa automaattisissa muutoksissa.

Toinen näkökohta on TDM-verkon joustava käyttö. Käyttäjien tarpeet vaihtelevat ajankohdan mukaan ja verkon tulee tukea muuttuvia käyttötapoja. Yhteyksien uudelleenreitityksen helppous ja nopeus on verkon palveluominaisuuksista tärkeimpien joukossa.

4.4.2 KONFIGURAATION MUUTOSTEN PRIRISOINTI

4.4.2.1 Ulkopuoliset toiminteet

Reitityksen automaattinen ohjaus ei puutu toiminteisiin, jotka eivät muuta verkon fyysistä tai loogista topologiaa. Loogisesti identtisen komponentin esim. suoran varayhteyden käyttöönotto voidaan suorittaa itsenäisesti.

4.4.2.2 Konfiguraatioon vaikuttavat toiminnot

Automaattinen verkonhallinta haluaa muutoksia tehtäväksi vianhallinnan tai toiminnan valvonnan ehdottamina. Syinä voivat olla mm. akuutti vika, ennustettu vikatilanne, kuorman tasaus ja laadullisesti paremman reitin käyttöönotto.

4.4.2.3 Toimintojen priorisointi

Verkonhallinnan eri toimintoryhmiltä vastaanotettavat vaateet saattavat olla ristiriitaisia, jolloin reitityksen ohjauksen tulee ratkaista suoritettavat muutokset. Pääpiirteissään priorisointi noudattaa seuraavaa järjestystä:

a) tietosuoja (korkein prioriteetti)

b) vian ohitus

c) toiminnan valvonta

d) tilanteen palautus / vianhallinta

e) erityisryhmien tarpeet

Manuaalinen verkonhallinta omaa aina korkeamman prioriteetin kuin automaattinen, joten erityisryhmien tarpeet saattavat nousta päällimmäisiksi.

4.4.3 KONFIGURAATION MUUTOKSET

4.4.3.1 Tehtävä

Käyttäjän toiminnan helpottamiseksi on TDM-verkkoa mahdollista muokata yksinkertaisesti sekä automaattisen että manuaalisen verkonhallinnan keinoin. Tietokantoihin sisällytetään konfiguraatiopaketteja, joiden mukaiseksi verkko ohjataan joko jonkin verkonhallinnalle määrätyn kriteerin tai käyttäjän itsensä ohjaamana.

4.4.3.2 Konfiguraatiopaketit

TDM-verkon jokaiselle portille on mahdollista kuvata kolme eri käyttömahdollisuutta. Näitä porttien ja yhteyksien kombinaatioita, konfiguraatiopaketteja, voidaan rakentaa käyttäjän tarpeiden mukaisesti.

Konfiguraatiota muutetaan joko käyttäjäliitännästä tai automaattisesti. Käyttäjäliitännässä muutoksen suorittajalta vaaditaan normaalit oikeudet. Automaattisesti uuden konfiguraatiopaketin käyttöönotto käy päinsä seuraavien kriteerien perusteella:

- ajankohta
- toisen verkonhallintajärjestelmän käsky

4.5 ERITYISRYHMIEN TARPEET

4.5.1 TAVOITTEET

Tarkoituksena on turvata mahdollisuudet, jotta voidaan huolehtia myöhemmin erikseen esille nousevista käyttäjäryhmistä ja niiden verkon toimintaan ja hallintaan liittyvistä vaatimuksista ilman ohjelmiston muutoksia. Näiden erityisryhmien tehtävät ovat selvästi rajattuja; niillä on selkeä tavoite ja tulos. Erityisryhmiin luetaan myös nykyisin tiedossa olevat vastaavanluonteiset tehtävät kuten laskutus ja ohjelmaversioiden kaukolataus.

4.5.2 TARPEIDEN ARVIOINTI JA TÄYTTÖ

Käyttöönoton jälkeen esille nousevat vajavaisuudet ja uudet mahdollisuudet muokata ja tutkia TDM-verkkoa ovat korkean tason toiminteita. Ne käyttävät hyväkseen jo olemassa olevia ominaisuuksia. Erityisryhmien palvelemiseksi tulee korkeimman prioriteetin omaavan TDM-verkon

käyttö- ja ylläpitohenkilökunnan pystyä luomaan uusia käyttäjäryhmiä, joille pätevät samat kriteerit kuin ohjelmiston peruspaketissa luoduille.

5. VIANHALLINTA

5.1 TEHTÄVÄ

Vianhallinnan tehtävä on tarjota toiminnot verkon tiedonsiirtokyvyn manuaaliselle ja automaattiselle ylläpitämiselle. Tämä tehtävä sisältää implisiittisesti vaatimuksen toimintakuntoisuuden tilan tuntemuksesta.

Vianhallinnan toiminnot jaetaan neljään ryhmään: vian havainnointi, vian paikallistus, vian ohitus ja alkuperäisen tilanteen palautus.

Tarkkailu- ja elvytystoimenpiteet ovat tosiaikaisia, pyrkimyksenä on säilyttää verkon kyky katkeamattomaan tiedonsiirtoon ennakoinnin avulla. Automatiikan tulee pystyä säilyttämään systeemin tila ja huolehtimaan siirrettävän datan eheydestä kaikissa olosuhteissa. Vianhallinta raportoi vikatilanteet hälytysten ja vikalokin muodossa sekä tarjoaa tiedot verkon tilasta verkonhallinnan muille toiminnoille ja muille verkonhallintajärjestelmille.

5.2 VIANHALLINNAN LIITYNTÄ MUIHIN VERKKOIHIN

Vianhallinan piiriin kuuluu myös verkonhallintaverkko mukaanlukien liitännät muihin järjestelmiin. Eri järjestelmien rajapinnoissa kuuluu vastuu toimintakuntoisuudesta hallinnollisesti näistä ylemmällä tasolla olevalle. Tämä vastuu koskee ainoastaan rajapintaa ja järjestelmät vastaavat muilta osin kokonaisuudessaan omasta toiminnastaan.

5.3 VIKOJEN ARVIOINTI

5.3.1 VIKATYYPIT

Verkossa esiintyvät tiedonsiirtoon vaikuttavat ongelmat voidaan jakaa äkillisiin ja asteittain muuttuviin. Näiden erityyppisten vikojen havainnointi ja jatkotoimenpiteet eroavat toisistaan.

Yht'äkkiset viat, esim. siirtotien katkeaminen on yleensä helppo paikallistaa riittävällä tarkkuudella vian ohittamiseksi. Vika havaitaan joko komponentin antaman ilmoituksen perusteella tai vianhallinnan suorittamissa testeissä. Tiedonsiirto katkeaa, mutta ohitus voidaan suorittaa suhteellisen nopeasti uudelleenreitityksen avulla, ottamalla käyttöön mahdollinen varayksikkö tai korjaamalla vika.

Haastavampi tehtävä on hiljalleen pahenevan ongelman tunnistaminen ja oikea reagointi siihen. Tälläisiä ovat esim. komponenttien lämpötilaongelmat ja ympäristöolosuhteista johtuvat tiedonsiirtovaikeudet. Näissä tapauksissa on pyrkimyksenä turvata tiedonsiirron jatkuvuus ilman käyttäjälle näkyviä katkoksia ja merkittäviä laadullisia ongelmia. Vianhallinta ei yksin pysty arvioimaan ilman historiatietojen analyysiä jonkin ongelman vakavuutta ja sen vaatimia toimenpiteitä. Yhteistyö käytönhallinnan kanssa pystyy sen sijaan tarjoamaan keinot ja suureet mittausten suorittamiseksi ja johtopäätöksien vetämiseksi. Verkon kunnosta vastaavan henkilökunnan osaaminen on merkittävällä sijalla ennakoivassa vikojen torjunnassa eikä automaattinen verkonhallinta yksin pysty toteuttamaan tätä toiminnetta.

5.3.2 VERKON KOMPONENTTIEN TOIMINNALLINEN LUOKITTELU

Vaatimiensa toimenpiteiden mukaan TDM-verkonhallinta luokittelee komponentit niiden toimintakelpoisuuden kannalta seuraaviin luokkiin:

a) Komponentti on täysin toimintakuntoinen.

b) Komponentin toimintakunto tai -varmuus on osittain heikentynyt tunnetusta syystä. Syyt saattavat olla myös sidoksissa aikaan tai tapahtumaan mutta tällöin toimintakunnon tulee olla ennustettavissa.

c) Epäluotettava komponentti, jonka toiminta on akuutisti tai kroonisesti epävarmaa. Tähän luokkaan ei komponentti saa kuulua kauaa, vaan jatkotesteillä se pyritään sijoittamaan johonkin muuhun luokkaan (ei luokkaan e).

d) Ei-toimiva komponentti. Tähän luokkaan kuuluvat myös komponentit, jotka on kytketty verkkoon mutta joita ei ole alustettu ja/tai testattu.

e) Tuntematon toimintakunto.

5.3.3 LUOKITTELUTASOT

TDM-verkonhallinnan kannalta tärkein tieto on verkon komponentin kykenevyys tiedonsiirtoon. Kaikille testeille on tuloksen osalta määrätty raja-arvo, joka jakaa testin kohteena olevan verkon komponentin (ja siten yhteyden jolla se sijaitsee) toimivaksi/ei-toimivaksi. Tämän li-

säksi määritellään raja, jolla komponentin toiminta näkyy käyttäjälle heikentyneenä palvelutasona. Tämä raja aiheuttaa komponentin luokituksen putoamisen luokkaan c. Jatkotestien perusteella komponentin luokitus muutetaan edelleen ja suoritetaan korjaustoimenpiteet, jos se on välttämätöntä.

5.4 VIAN HAVAINNOINTI

5.4.1 TAVOITE

TDM-verkossa tai siihen liitetyssä tiedonsiirtoverkossa oleva vikatilanne saadaan TDM-vianhallinnan tietoon viestin, aktiivisen testauksen tai käyttäjäliitynnän kautta. Tarkoituksena on löytää ongelma mahdollisimman nopeasti ja sellaisella tarkkuudella, että vian paikallistuksessa on tarkennuksen kohteena tietty tiedonsiirtoyhteys. Tällöin vian ohitus ja paikallistus voivat olla rinnakkaisia toimintoja ja vikojen vaikutus tiedonsiirtokykyyn pienenee. Kiinteällä yhteistyöllä käytönhallinnan kanssa vianhallinta pystyy havaitsemaan luotettavuuden kannalta verkon kriittiset kohdat ja siten parantamaan palvelutasoa.

5.4.2 TESTAUS

Testien avulla pysytään selvillä verkon komponenttien (laitteiden ja siirtoteiden) toimintakunnosta ja laadusta. Vianhallinnan toiminnoista sekä vian havainnointi että paikallistus käyttävät hyväkseen näitä testejä. Testit jaetaan kahteen ryhmään; itsetestit ja testisilmukat. Niiden kattamat alueet ovat osittain päällekkäiset, mutta käyttöalueiden erot hyötyvät tästä.

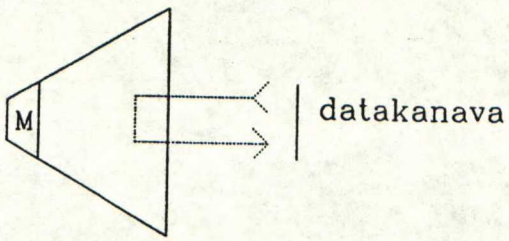
TDM-vianhallinnan on pystyttävä hyödyntämään kaikki verkon komponenttien suorittamat testit, mikäli niistä on mahdollista saada uutta tietoa.

5.4.2.1 Itsetestit

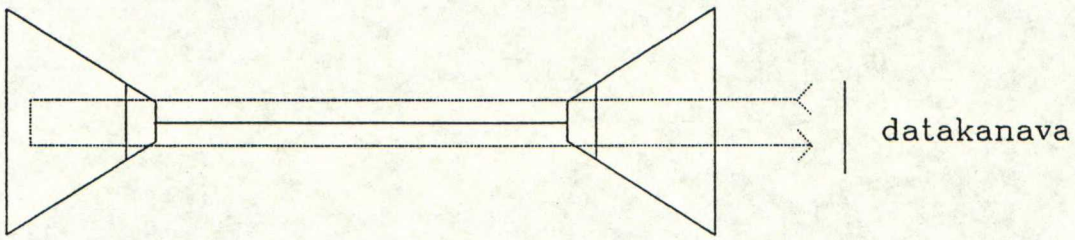
Itsetestejä käytetään aina varmistettaessa laitteen kunto käyttöönoton yhteydessä sekä vian paikallistuksen tarkentamiseen. Laitteiden sisäänrakennetun logiikan avulla ne voivat itsenäisesti havaita ja paikallistaa viallisen toiminnallisen ja fyysisen yksikön. Koska verkon komponenttien itsetestiominaisuudet ja -tarkkuus vaihtelevat, täytyy TDM-verkonhallinnan olla selvillä kunkin komponentin erityispiirteistä.

5.4.2.2 Testisilmukat

Testisilmukoiden avulla tarkistetaan siirtoyhteyksien toimintakunto ja laatu. Siten niiden avulla tarkistetaan myös komponenttien sisäinen toiminta tiedonsiirtoominaisuuksien osalta. TDM-verkon komponenttien omien testisilmukoiden lisäksi pitää aikajakoisen multiplekserin MUX64k:n kyetä toteuttamaan CCITT:n suosituksessa X.150 määritellyistä testeistä sellaiset, että ne yhdessä kattavat koko tiedonsiirtoreitin yhden kanavan osalta. Testikombinaatioksi valitaan CCITT:n suosituksen X.150 testit 2b ja 3c.



Kuva 13. Testi 3c. päätelaitteen ja MUX64k:n paikallistesti, päätelaitteelle lähetetään takaisin siltä vastaanotettu bittikuvio.



Kuva 14. Testi 2b. multipleksereiden välinen testi kanavatasolla, testin aloittaneen multiplekserin lähettämä bittikuvio lähetetään sille takaisin. Bittikuvio voidaan lähettää joko aloittavalta multiplekseriltä tai päätelaitteelta.

Silmukkatestien vaatimat testikuviot voidaan lähettää joko johonkin verkon porttiin kytketystä erillisestä testilaiteesta tai TDM-verkonhallinnan sisäisestä testigeneraattorista. Testigeneraattorin lähettämän ja vastaanotossa tarkistaman testikuvion avulla voidaan testata kaikkia kanavia kerrallaan. Mikäli käytössä on ulkoinen testilaite on testi suoritettava manuaalisesti eivätkä testien tulokset tallennu automaattisesti vaan ne pitää syöttää TDM-verkonhallinnalle käyttäjäliitynnästä.

5.4.2.3 Testien suoritus

Seuraavassa on esitetty tavat, joilla testit voidaan aloittaa ja lopettaa. Tavat koskevat kaikkia testityyppejä ja niitä voidaan käyttää kaikkina mahdollisina kombinaatioina. Myös parametrit ovat muutettavissa testien tuloksien seurauksena, esim. silmukkatestien välistä aikaa voidaan automaattisesti pienentää mikäli testituloksien varianssi kohoaa yli manuaalisesti annetun arvon.

Testien aktivointi: (p = parametrisoitavissa)

Käyttäjäliitynnästä
Käytönhallinnan komento
Kellonaika (p)
Määrätyin väliajoin (p)

Testien lopetus: (p = parametrisoitavissa)

Käyttäjäliitynnästä

Käytönhallinnan komento

Kellonaika (p)

Testin ajallinen kesto (p)

Testikuvion pituus (testisilmukat) (p)

Bittivirhesuhteen ylitys (p)

Epäonnistuneitten yritysten lukumäärä (p)

Peräkkäisten epäonnistuneitten yritysten lukumäärä (p)

5.4.3 VIKAILMOITUKSET

5.4.3.1 Vikailmoituksen avaaminen

TDM-verkonhallinnan vianhallinta keskustelee jatkuvasti kaikkien TDM-verkkoon kytkettyjen laitteiden ja muiden verkonhallintajärjestelmien kanssa. Vikailmoitus voidaan antaa myös käyttäjäliitynnästä. Kaikissa näistä tapauksista ja vianhallinnan havainnoidessa vian luodaan ja avataan TDM-verkonhallinnalle vikaraportti.

5.4.3.2 Vikailmoituksen sulkeminen

Vikailmoitus suljetaan, kun joko on palautettu alkuperäinen tilanne tai stabiloitu uusi tilanne; esimerkiksi käyttöönotettu sekundaarireitti määritellään primaariksi. Mikäli stabiloidaan uusi tilanne täytyy suorittaa uudelleenmäärittely koskien primaari- ja sekundaariyhteyksiä.

5.4.3.3 Vikailmoituksen sisältö

1. Ilmoitusta koskevat tiedot
- avausajankohta
- ilmoittava komponentti/henkilö
- ilmoituksen vastaanottaja (mikäli ilmoitusta ei annettu käyttäjäliitynnästä)
- sulkemisajankohta
- sulkemisen suorittanut henkilö

2. Vikaa koskevat tiedot
- havainnointiajankohta
- sijainti
- vian luokittelu
- suoritetut testit tuloksineen
- korjaustoimenpiteet

3. Vian ohitusta koskevat tiedot
- vian ohitushetki
- uusi reitti/komponentti
- mikäli stabiloidaan uusi tilanne lisäksi:
    - varareitti

4. Alkuperäisen tilanteen palautus
- ajanhetki
- suorittanut henkilö

5. Käytöstä vastaavan henkilökunnan vapaamuotoisille ilmoituksille varattu kenttä

5.4.4 ONGELMIEN ENNUSTAMINEN

Vaikeutena on johtopäätösten vetäminen seurausten, ei varsinaisten syiden perusteella. Seuraukset ovat mitattavissa vianhallinnan suorittamilla testeillä ja muilla mittareilla kuten saatavuus. Komponentin vikaluokittelu "epäluotettavaksi" aiheuttaa päätöksen jatkotesteistä. Pääasiallisesti ennakoivat toimenpiteet kuuluvat käytönhallinnalle.

5.4.5 HÄLYTYSTASOT JA JATKOTOIMENPITEET

Komponenttien luokittelun yhteydessä määritettiin luokat: "epäluotettava" ja "ei-toimiva". Nämä molemmat indikoivat ratkaisevasti heikentyneestä toimintakunnosta ja johtavat elvytystoimenpiteisiin. Riippuen alustavien testien ja ilmoitusten tarkkuudesta siirrytään vian ohitukseen joko suoraan tai paikallistuksen kautta.

5.5 VIAN PAIKALLISTAMINEN

5.5.1 TARKKUUS SIJAINNIN SUHTEEN

Vianhallinnan vaatimukset paikallistuksen tarkkuudelle liittyvät suoraan vian ohituksen vaatimuksiin; mitkä yksiköt ovat automaattisesti korvattavissa joko reitityksen muutoksella tai varayksikön käyttöönotolla? Tarkkuusvaatimuksia nostavat ylläpidon ja käytönhallinnan tarpeet, huolto ja vikaantumistiheyksien arviointi vaativat tiedon yksittäisen fyysisen ja toiminnallisen kokonaisuuden tarkkuudella.

5.5.2 TARKKUUS VAKAVUUDEN SUHTEEN

Päämääränä on komponentin lopullinen sijoittaminen vikakategorioihin ja päättäminen mahdollisista jatkotoimenpiteistä. Koska verkonhallintajärjestelmältä ei voida olettaa kovin laajaa tietämystä, ei komponenttia sijoiteta automaattisesti luokkaan "osittain heikentynyt toimintakunto".

5.5.3 MENETELMÄT

Vian paikallistukseen käytetään samoja keinoja kuin vikojen havainnointiin; testejä ja ilmoituksia.

5.6 VIAN OHITUS

5.6.1 EDELLYTYKSET

TDM-verkon kyky ohittaa havaittu vika riippuu pitkälti kyseessä olevan verkon topologiasta ja konfiguraatiosta; miten siinä on varauduttu esiintyviin ongelmiin. Vianhallinnan tehtävä on yhdessä käytönhallinnan kanssa määrätä käyttöönotettavaksi sopivin keino tiedonsiirron jatkamiseksi.

5.6.2 MENETELMÄT

Vian ohituksen menetelmät prioriteettijärjestyksessä ovat: reitityksen muutos, varayksikön käyttöönotto ja vian korjaus. Reitityksen muutos on nopein tapa jatkaa tiedonsiirtoa. Se ei vaadi kovin tarkkaa paikallistusta ja proseduuri on nopea suorittaa, onhan varareitti jatkuvan testidatan siirtotie. Varayksikön käyttöönotto sen sijaan vaatii nopeaa ja tarkkaa vian paikallistusta sekä saattaa vaatia aikaavieviä alustustoimia. Varayksikön käyttöönotto on kuitenkin lähin vaihtoehto alkuperäiselle tilanteelle ja se voidaan määrätä ensisijaiseksi vianohitusmenetelmäksi.

5.6.3 REITITYKSEN MUUTOS

Reitityksen muutos voidaan suorittaa joko käyttäjäliitynnästä tai vianhallinnan toimesta, käyttäjäliitynnästä suoritettava valinta on aina määräävä ristiriitaisissa tilanteissa. Vianhallinnassa määrätään kullekin tiedonsiirtoyhteydelle ensisijainen varayhteys. Mikäli tämä ei ole käytettävissä valitaan reitti seuraavien kriteerien perusteella:

1. Yhteyden tarjoama kapasiteetti. Mikäli kapasiteettia ei kuitenkaan ole riittävästi valitaan keskeytettävät yhteydet porttien prioriteettien perusteella.

2. Yhteyden laatu. Käytönhallinnasta saadaan selville kunkin yhteyden historiatiedot ja niiden perusteella arvioitu laatu.

3. Muiden yhteyksien primaarista varatietä ei valita muulloin kuin sen ollessa ainoa mahdollisuus.

4. Yhteyden suoruus. Tasavertaisista varareiteistä otetaan käyttöön se, joka kulkee vähimpien komponenttien kautta.

5. Tietosuoja. Suojauksenhallinta voi sulkea jonkin yhteyden pois käytöstä, suojauksenhallinnan määräykset ovat ehdottomia.

6. Yhteyden hallittavuus. Edellä mainittujen kriteerien perusteella tasavertaisista reiteistä valitaan verkonhallinnallisesti älykkäämpien komponenttien muodostama reitti. Valintaperuste on heikoimman komponentin älykkyys.

5.7 ALKUPERÄISEN TILANTEEN PALAUTUS

5.7.1 PÄÄTÖKSENTEON LÄHTÖKOHDAT

Vikaantumista edeltäneen tilanteen palauttamisessa ei ole yleispätevää sääntöä, vaan kukin tapaus pitää arvioida erikseen tässä esitettyjen kriteerien perusteella. Usein päätöksenteko jätetään verkon kunnosta vastaavan henkilökunnan harkittavaksi. Nyt esitetyt kriteerit perustuvat olettamukselle, että reitit on verkkoa konfiguroitaessa määritelty eriarvoisiksi. Mikäli näin ei ole käytetään tietysti laadultaan parempaa siirtoreittiä.

Ehdoton ehto on tietysti korjatun primaarireitin laatu. Siirtoyhteys testataan päästä-päähän ulottuvalla silmukkatestillä ja kaikki yhteydellä olevat laitteet suorittavat itsetestin. Lisäksi arvioidaan his-

toriatiedoista yhteyden vikaantumistiheys. Kumman tahansa kriteerin pettäminen estää välittömän käyttöönoton. Automaattista reitityksen muutosta ei suoriteta mikäli tiedonsiirto keskeytyy.

5.7.2 KRITEERIT

Edellisessä luvussa kuvattiin staattiset ehdot, muiden ehtojen painoarvoa voidaan muuttaa verkon konfiguraation mukaan. Näitä ovat:

a) Erot käyttökustannuksissa.
b) Erot kapasiteetissa (kapasiteettitarve huomioitava)
c) Erot tietoturvallisuudessa
d) Muiden verkonhallintajärjestelmien vaatimukset
e) Kuinka paljon varareitti varaa muiden yhteyksien kapasiteettiä
f) Erot siirron laadussa (virheettömyys, vasteajat)
g) Erot yhteyksien hallittavuudessa

5.8 RAPORTOINTI

Vianhallinta raportoi verkon kunnosta ja omista toimistaan sekä verkonhallinnan muille toiminnoille että käyttäjäliityntään. Muiden toimintojen tarpeita varten se pitää itsenäisesti yllä konfiguraationhallinnan tietokantoja verkon komponenttien toimintakuntoisuuden osalta.

5.8.1 HÄLYTYKSET

Kaikki verkon komponentit lähettävät hälytykset keskitettyyn verkonhallintaan. Keskitetyssä verkonhallinnassa suoritetaan hälytysten rekisteröinti ja talletus. Rekisteröinnin perusteella päätetään tulostetaanko ko. hälytys käyttäjäliitynnässä vai ei. Hälytykset jaetaan rekisteröintiä varten seuraaviin luokkiin:

I Kriittinen - Verkon toiminta on rajoittunutta

II Ei-kriittinen - Verkon toiminta on rajoittunutta osittain

III Informatiivinen - Verkon toiminta ei ole rajoittunutta

Luokan I hälytykset tulostetaan aina käyttäjäliitynnässä, luokkien II ja III hälytykset voidaan valita tulostettaviksi.

5.8.2 VIKALOKI

Käyttäjäliityntään tila ja toimet indikoidaan pitämällä vikalokia, josta käyvät ilmi myös verkon komponenteilta tulleet hälytykset. Se on verkonhallintajärjestelmän ja sitä käyttävän henkilökunnan välinen kommunikaatiomenetelmä, johon taltioidaan verkon epänormaalit tapahtumat ja reagointi niihin.

6. KONFIGURAATIONHALLINTA

6.1 TEHTÄVÄ

Konfiguraationhallinta tarjoaa funktiot, joiden avulla voidaan kerätä, ylläpitää ja luovuttaa tietoa verkon konfiguraatiosta sekä muuttaa sitä. Konfiguraatiolla käsitetään: Verkon laitteisto, niiden väliset fyysiset ja loogiset yhteydet sekä liitännät ulkomaailmaan. Konfiguraationhallinnan funktiot rajoittuvat viimeisimmän tiedon ylläpitoon ja välitykseen; historiatietojen keräys ja johtopäätösten teko niiden pohjalta ei kuulu konfiguraationhallinnalle. Verkonhallinnan toiminnoista ainoastaan konfiguraationhallinta tarjoaa funktiot verkon tilan muuttamiseksi.

6.2 VAATIMUKSET

Konfiguraationhallinnan tehtäville asetetaan vaatimukset verkonhallinnan muissa toiminnoissa, verkkoon liittyvissä muissa tiedonsiirto- ja verkonhallintajärjestelmissä sekä verkon eri käyttäjäkunnissa. Tässä luvussa tarkastellaan TDM-verkon konfiguraationhallinnan vaatimuksia näihin näkökulmiin pohjautuen, vaatimusten pohjalta määritellään luvun myöhemmissä kappaleissa:

a) Tietokantojen sisältö ja jaottelu

b) Toiminnot liittyen: Komponenttien käyttöönottoon, tilan ja toiminnan muuttamiseen sekä käytöstä poissulkemiseen

6.2.1 TDM-VERKONHALLINNAN MUIDEN TOIMINTOJEN VAATIMUKSET

Aikaisemmissa luvuissa esitetyt vaatimukset voidaan tiivistää seuraaviksi pääkohdiksi:

- Tietämys verkon kaikista komponenteista, niiden toimintatilasta ja -kunnosta sekä komponenttien välisistä fyysisistä yhteyksistä. Kaikista näkökulmista kerätään sekä nykytilanne että kunkin laitteen ja yhteyden potentiaaliset toiminnot esim. testimahdollisuudet.

- Kyky kommunikoida kaksisuuntaisesti kaikkien TDM-verkon komponenttien ja TDM-verkkoon liittyvien järjestelmien kanssa.

TDM-verkko voidaan kytkeä muihin tietoliikenne- ja verkonhallintajärjestelmiin; Tietämyksen liitetystä järjestelmästä ja kommunikaation sen kanssa tulee olla riittävä tietoliikenteen ja vikadiagnostiikan tarpeisiin. TDM -verkonhallinnalla tulee lisäksi olla tietämys liitännästä, järjestelmien välisestä hierarkiasta ja prioriteeteista kummankin järjestelmän suhteen.

6.2.2 VERKON KÄYTTÄJIEN VAATIMUKSET

Kerättävät ja ylläpidettävät tiedot liittyvät TDM-verkon ylläpidon ja jatkokehityksen piiriin. Tarkoituksena on kehittää yhtenäisyyttä ja helpottaa tiedon keruuta. Automaattisen verkonhallinnan akuuttien tarpeitten lisäksi tarvitaan kustakin laitteesta hallinnollista tietoa. Ylläpidon ja huollon toimia helpottaa myös muutosja versionhallinnan toteuttaminen etäisvalvonnalla.

Verkkoon ja sen toimintaan kohdistuvat funktiot ovat samat kuin on määritelty automaattisen verkonhallinnan toiminnoiksi vian-, käytön-, suojauksen- ja laskutuksenhallinnoissa. Lisäfunktiot koskevat käyttöönottovaihetta. Näitä ovat: Komponentin asennus-toimenpiteet koskien sekä komponenttia itseään että verkonhallintaa.

6.3 TIETOKANNAT

6.3.1 TIETOKANTOJEN SISÄLTÖ

Tietokantojen sisältö muokkautuu edellisessä luvussa esitettyjen seikkojen perusteella. Tässä luvussa määritellään tietokantojen koko sisältö eli kaikki se, mikä mahdollisesti näkyy ulospäin sekä on verkon sisäisessä käytössä.

6.3.2 TIETOKANTOJEN JAKO

Tietokantojen sisällön jaon pääkriteerejä ovat tietosuoja ja käyttötarkoitus (käyttäjäryhmä). Jaottelu tukee portaittaista toteutusvaihetta eikä saa aiheuttaa raskautta tietokantojen ylläpidossa. Muita rajaviivoja osien välille vetävät tietojen: stabiilius, kattavuus ja ajallinen kesto.

TDM-verkon kuvaus jaetaan seuraaviin pääluokkiin:

(I) Varsinaisesti konfiguraationhallinnan ulkopuolella on nimeämiskäytännön kuvaus. Se liittyy kuitenkin välttämättömänä osana loogisen ja fyysisen rakenteen esitykseen, joten se esitetään tässä yhteydessä.

(II) Ympäristökuvaus, jossa määritetään TDM-verkon verkonhallinnallinen asema ympäröivissä ja alemman tason systeemeissä. Olennaista tietoa ovat hierarkioiden ja prioriteettien esitys.

(III) TDM-verkon kuvaus, jossa on esitetty verkon looginen rakenne, myös muiden tietoliikenneverkkojen kautta kulkevat tai niihin päättyvät yhteydet.

(IV) TDM-verkonhallinnan kuvaus mukaanlukien verkonhallintaverkko ja käyttäjien prioriteetit.

(V) Verkon komponenttien kuvaus, mikä sisältää myös kuvaukset hallinnollisesti TDM-verkon ulkopuolisista mutta tietoliikenteellisesti siihen kuuluvista komponenteista.

6.3.2.1 NIMEÄMISKÄYTÄNTÖ

Tarkoituksena on määrittää tapa, jolla voidaan yksiselitteisesti ilmaista TDM-verkon komponenttien liitännät ja suhteet. Nimeämiskäytäntö on voimassa verkon sisällä ja riippuen kytkennöistä muihin verkkoihin myös käyttäjäliitynnässä. Mikäli TDM-verkonhallinta on korkein verkonhallintaelin käytetään tätä nimeämiskäytäntöä.

Nimeämistä varten verkko jaetaan seuraaviin verkonhallinnollisiin hierarkiatasoihin:

1. Verkko

Suurin itsenäinen kokonaisuus, jota voidaan hallita yhdestä TDM-verkonhallinnan pisteestä. TDM-verkko liittyy usein sekä tietoliikenteellisesti että hallinnollisesti ylempään tietoliikennejärjestelmään.

2. Osaverkko (optionaalinen)

TDM-verkon itsenäinen osa, joka voidaan sekä hallinnollisesti että tietoliikenteellisesti irroittaa TDM-verkosta vaikuttamatta kyseisen osaverkon sisäisiin tietoliikenneyhteyksiin.

3. Solmu

Yhden MUX64k:n ja siihen mahdollisesti liittyvien komponenttien muodostama kokonaisuus.

4. Komponentti

Toiminnallinen kokonaisuus, joka suorittaa jonkin tietoliikenteellisen tai verkonhallinnallisen toiminnon.

5. Osakomponentti

Komponentin itsenäisesti kontrolloitavissa oleva tai tietoliikenteellisesti oleellinen yksikkö.

Kaikki komponentit nimetään yksiselitteisesti sen ketjun mukaan mihin se verkonhallinnan hierarkiassa kuuluu. Osaverkko on optionaalinen riippuen verkon laajuudesta.

Verkon (osa-) ja komponentin (osa-) nimestä tulee ilmetä:

a) Tyyppi
b) Tunnus
c) Ylempi elin

6.3.2.2 YMPÄRISTÖKUVAUS

Ympäristökuvaus sisältää TDM-verkonhallinnan liittymisen muihin mahdollisiin verkonhallintajärjestelmiin. TDM-verkonhallinta voi sekä olla itse osa suurempaa kokonaisuutta että hallita jotain mahdollisesti jopa tietoliikenteellisesti irrallista järjestelmää.

Ympäristökuvaus ilmaisee kunkin liitettävän järjestelmän kohdalla:

a) Nimi, josta ilmenee järjestelmän tyyppi ja tunnus
b) Järjestelmän oikeudet TDM-verkossa
c) TDM-verkonhallinnan oikeudet liitettävässä järjestelmässä
d) Looginen liityntäpiste(-et)

6.3.2.3 VERKON KUVAUS

Verkon kuvaus sisältää ne tietoliikennekytkennät, jotka verkon eri komponenttien välillä ovat sekä fyysisesti että loogisesti. Tässä ilmaistaan:

a) Verkon komponenttien fyysiset liitännät tietoliikenneteihin ja muihin komponentteihin.

b) Porttien väliset loogiset liitännät ja reitit sekä näiden reittien varareitit.

c) Kohtien a) ja b) mukaiset tiedot TDM-verkon ja muiden verkkojen välisistä tiedonsiirtoyhteyksistä.

d) Pelkästään verkonhallinnan käytettävissä olevat fyysiset ja loogiset yhteydet muihin verkkoihin.

6.3.2.4 TDM-VERKONHALLINNAN KUVAUS

TDM-verkonhallinnan kuvaus jaetaan seuraaviin näkökulmiin:

a) Verkonhallintaverkon kuvaus kohdan (III) mukaisesti.

b) Verkonhallintaan osallistuvien elimien oikeudet. Oikeudet määritetään toiminteittain yhteys- ja komponenttikohtaisesti.

6.3.2.5 VERKON KOMPONENTTIEN KUVAUS

Kustakin verkon komponentista mm. välitin-, keskitin-, kytkentä- että verkonhallintalaitteista ja siirtoteistä luodaan ja ylläpidetään seuraavia tiedostoja soveltuvin osin:

a) Yleiset tiedot

- nimi
- omistava organisaatio
- nykyinen sijainti
- vastuuhenkilö yhteystietoineen

b) Asennus- ja ylläpitotiedot

- asennuspvm ja asennuksen suorittanut henkilö
- kokoonpano pienimmän konfiguroitavan yksikön tarkkuudella
- laitteen ja sen kunkin konfiguroitavan yksikön ohjelmisto- ja laiteversiot
- ohjelmisto- ja laiteversioiden historiatiedot
    - muutettu versio
    - muutospvm
    - muutoksen suorittanut henkilö

c) Liitäntä- ja asetustiedot

- kaikki fyysiset kytkennät
- muutettavissa olevat asetustiedot kuten siltaukset ja kanavanopeudet kaikilta osin

d) Testaustiedot

- kaikki laitteen testimahdollisuudet
- kustakin tulosten tulkinta - toimintakuntoisuuden luokittelurajat

e) Komponentin tila ja kunto

- onko laite käytössä, testattavana vai kytketty pois käytöstä
- viimeisimpien testien perusteella tehty luokittelu

f) Kytkentätiedot

- loogiset yhteydet reittitietoineen
- sallitut yhteydet kytkentäisissä tapauksissa
- primaariset varareitit
- reittien tila ja kunto
- reittien tietosuojaluokittelu

6.3.3 TIETOKANTOJEN SIJOITUS

6.3.3.1 Vaatimukset

Peruslähtökohta on luotettavuus; tietojen tulee olla häipymättömässä muistissa, ei koskaan yhden komponentin varassa ja aina saatavilla. Ristiriidassa tämän vaatimuksen kanssa on verkonhallinnalle tarpeellisten tiedostojen ja tietoliikenteen keveys. TDM-verkko käyttää kontrollitietojen siirtoon varsinaiselle tietoliikenteelle varattua kapasiteettia ja kuormitus on pois varsinaiselta hyötyliikenteeltä. Varmistavissa tiedostoissa ei ole tarkoituksenmukaista ylläpitää tosiaikaista tietoa usein muuttuvien parametrien arvoista.

6.3.3.2 Komponenttikohtaisten tietokantojen sisältö

Varsinainen sijoitus suoritetaan hajautetusti sisällön mukaisen jaottelun perusteella. Kukin komponentti säilyttää kaikki sille määrätyt konfiguraatio- ja statistiikkatiedot. Kappaleen 6.3.2 käyttämän jaon mukaisesti näitä konfiguraatiotietoja ovat kohdan 6.3.2.5 tiedot. Verkonhallinnan toimintoja varten vaadittavia tietoja ovat myös kohdan 6.3.2.4 mukaiset tiedot.

Kuhunkin komponenttiin fyysisesti liittyvistä alemman tason komponenteista (kohdassa 6.3.2.5 c)) määritellyt liitännät) tulee tietää näiden konfiguraatio- ja testaustiedot; 6.3.2.5 d) ja 6.3.2.5 e).

Loogisesti vastaavan tasoiset komponentit ovat tietoisia edellisten tietojen lisäksi kohdan 6.3.2.5 f) mukaisista reitityst ä ohjaavista parametreista.

Verkonhallintalaitteisto ylläpitää tietokantoja kaikista verkon komponenteista. Jotta ylläpito ei olisi työlästä, säilytetään keskitetysti ainoastaan staattisia tietoja: 6.3.2.5 c) ja 6.3.2.5 d) sekä 6.3.2.5 b) kohdasta tämän hetkiset ohjelmisto- ja laitteistoversiot sekä laskutustiedot. Kokonaiskuvan saamiseksi täytyy verkonhallinnalla olla tietysti tietämys koko verkosta; eli kohtien 6.3.2.2, 6.3.2.3 ja 6.3.2.4 mukaiset tiedot.

6.4 KONFIGURAATIONHALLINNAN TOIMINNOT

6.4.1 KOMMUNIKOINTI VERKONHALLINNAN MUIDEN TOIMINTOJEN KANSSA

Kaikki verkon statukseen kohdistuvat toiminnot tapahtuvat konfiguraationhallinnan toimesta ja se tarjoaa yhtenäisen rajapinnan muille verkonhallinnan funktioille. Tämän rajapinnan läpi kommunikointi tapahtuu suoraan tietokantaan kohdistuvan protokollan välityksellä. Konfiguraationhallinta huolehtii välitettävän tiedon validiteetista kappaleen 6.4.4 mukaisesti. Mikäli olemassaoleva tieto ei vastaa vaatimuksia joko tarkkuudeltaan tai uutuusarvoltaan tulee konfiguraationhallinnan päivittää tieto.

Toiminnekohtaisella oikeuksien tarkistamisella turvataan tietosuoja kappaleessa 3.2.5 määritellylle tasolle.

6.4.2 KOMMUNIKOINTI MUIDEN VERKONHALLINTAJÄRJESTELMIEN KANSSA

Kommunikointi muiden verkonhallintajärjestelmien kanssa ei eroa edellisen kappaleen periaatteista; konfiguraationhallinta toimii keskitetysti ainoana ulospäin kommunikoivana TDM-verkonhallinnan toimintona.

TDM-verkonhallinnan ja ylempien verkonhallintajärjestelmien väliset kommunikointitarpeet liittyvät TDM-verkon toiminteisiin. Tällöin voidaan ylemmälle järjestelmälle määritellä sen valvottavana tai hallittavana oleva tehtäväkenttä. Tehtäväkenttä koostuu osajoukosta TDM-verkonhallinnan toimintoja, on myös mahdollista siirtää kokonaisvastuu ylemmälle järjestelmälle.

Mikäli TDM-verkonhallinta toimii ylempänä verkonhallintajärjestelmänä muille järjestelmille, tulee se toimimaan edellisen kappaleen mukaisesti.

6.4.3 KOMMUNIKOINTI VERKON KOMPONENTTIEN KANSSA

Kommunikointi verkon komponenttien kanssa liittyy:

a) Komponentin käyttöönottoon
b) Komponentin tilan ja toiminnan tiedusteluun
c) Komponentin tilan ja toiminnan muutokseen
d) Komponentin sulkemiseen pois käytöstä

Näistä kohdat a) ja d) sekä tietyissä tilanteissa c) saavat aiheuttaa tietoliikenteen keskeytymisen.

Kommunikointiin verkon komponenttien kanssa liittyy automaattinen tietokantojen ylläpito. Suoritetun toimenpiteen jälkeen tulee tietokannat päivittää. Verkon kukin komponentti mukaanlukien keskitetty verkonhallinta vastaa oikean arvon päivittämisesta omissa tiedostoissaan sekä siihen liitettyjen komponenttien tiedostoissa.

Tietueen mahdollinen luominen tai poistaminen suoritetaan uuden komponentin käyttöönoton tai sellaisen poistamisen yhteydessä.

6.4.4 TIETUIDEN LUOMINEN

Tietokantoihin luodaan tarvittavat tietueet konfiguraationhallinnan vastaanottamasta vaatimuksesta. Tämä vaatimus voi olla joko epäsuora liittyen tietueen sisältöön tai suora liittyen tietueen edustaman komponentin syntymiseen tai poistumiseen.

Tietueen luomiseen liittyy sen toiminnan määrittely. Tietueelle ja sen eri kentille määrätään:

a) Päivitysoikeudet
b) Poistamisoikeudet
c) Päivitysaktiivisuus (6.4.5)

a) Päivitysoikeudet myönnetään tietueille kenttäkohtaisesti. Tietueen luonut prosessi voi myös päivittää kaikkia sen kenttiä. Muutoin verkonhallinnan prosessit voivat päivittää ainoastaan kenttiä, joiden sisältöön ne vaikuttavat myös toiminnallisesti. Manuaalisella verkonhallinnalla on oikeudet verkon ja sen komponenttien staattisiin tietoihin.

b) Poistamisoikeudet on tietueen luoneella prosessilla ja manuaalisella verkonhallinnalla.

6.4.5 TIETOKANTOJEN YLLÄPITO

Tietokantojen sisältöä ylläpidetään kolmella aktiivisuustasolla:

a) Automaattisesti tiedon vanhennuttua parametrikohtaisen raja-arvon perusteella.

b) Konfiguraationhallinnalta pyydetyn palvelun tuloksen mukaisesti.

c) Konfiguraationhallinnan välittämän palvelun tuloksen perusteella.

Kohdan a) mukainen parametri voidaan liittää kaikkiin luotaviin kenttiin. Kustakin kentästä vastaava verkonhallinnan toiminto vastaa myös tiedon päivityshetkestä. Tälläisiä kenttiä ovat esim. komponenttien toimintakunto.

Kohtien b) ja c) vaatimat tehtävät tulevat suoritetuiksi automaattisesti. Kunkin konfiguraationhallinnan suorittaman toiminnon vastaanottamaa tai välittämää arvoa verrataan tietokantojen vastaavaan ja jälkimmäinen päivitetään tarvittaessa.

6.4.6 TIETUEIDEN POISTAMINEN

Tietue poistetaan aktiivisesta tietokannasta, kun sen edustama verkon komponentti poistetaan käytöstä. Tietueen sisältö siirretään ei-aktiiviseen tietokantaan, jossa sen eri kenttiin voidaan viitata kuten aktiivisessa tietokannassa. Tietueen eri kenttien sisältö jäädytetään tietueen poistamishetkellä.

7. YHTEENVETO

Kansainvälisen standardointijärjestön ISO:n verkonhallinnan OSI malli määrittelee tiedonsiirtoverkon verkonhallinnan toiminnot. Malli jaottelee tiedonsiirtoverkon verkonhallinnan toiminnot osa-alueisiin, mutta ei ota kantaan niiden toteutukseen.

Työssä tarkasteltu tiedonsiirtoverkko on verkonhallinnallisesti selkeä. Se koostuu tehtäviltään ja toiminnoiltaan rajatuista verkon komponenteista, joitten valvonta ja hallinta jaetaan sisäisiin ja ulkoisiin toimintoihin. Sisäiset, komponenttien itsensä suorittamat, toiminnot vastaavat verkon tiedonsiirtokyvystä myös yksinkertaisissa vikatilanteissa. Ulkoiset, erillisen verkonhallintalaitteiston toteuttamat, toiminnot optimoivat verkon toiminnan sekä lyhyellä että pitkällä tähtäimellä. Vastuun ja toimintojen hajauttaminen verkon päätehtävästä, tiedon siirtämisestä, parantaa sen toimintavarmuutta. Keskitetyn ulkoisen verkonhallinnan kuorma ei myöskään nouse liiaksi vaikeuttaakseen verkon laajennettavuutta.

Aikajakoiseen multipleksointitekniikkaan perustuva tiedonsiirtoverkko voi toimia sekä täysin itsenäisenä että osana laajempaa verkkoa. Erityisen jälkimmäisessä tapauksessa on tärkeätä yhdistää TDM-verkonhallinta ylemmän tason verkonhallintajärjestelmään. TDM-verkon rajapintana muihin järjestelmiin toimii erillinen verkonhallintajärjestelmä . Tämä rajapinta on määritelty OSI verkonhallinnan mallissa ja tulee olemaan yleisesti käytetty erilaisten järjestelmien yhdistämisessä.

Älykkyyden hajauttaminen selkeyttää järjestelmän keskitetyn osan käyttäytymistä ja käyttöä. Seikka, jolla on arvoa informaatiojärjestelmien monipuolisuuden ja -mutkaisuuden kasvaessa. Samoin se helpottaa näiden toimintojen automatisointia. Keskitetyn osan tehtäviin kuuluu tiedon kerääminen ja jalostaminen päättelyä varten. Tiedonsiirtoverkkojen kompleksisuutta kasvattaa riippuvuus ympäröivistä järjestelmistä ja häiriöalttius. Oppivat asiantuntijajärjestelmät eivät ole vielä hyödynnettävissä, mutta vastaavat periaatteiltaan verkonhallinnan vaatimuksia. Tiedonsiirtoverkon voidaan ajatella olevan virtuaalinen moniprosessorijärjestelmä, jossa ihmisen tehtävänä on olla käynnistäjä ja valvoja.

LÄHDELUETTELO

/1/ "Mackintosh" Yearbook
Electronics Data 1987,
Benn Electronics
Vol. 1, ss 73-78

/2/ Rahko Kauko
Puhelintekniikka II:3
Tietokoneohjaus ja verkot
TKY moniste 343 1974, s 43

/3/ Network control and management systems
International Data Corporation, 1987

/4/ Network management and performance measurement
International Data Corporation, 1987

/5/ All about network management systems
Datapro research corporation, 1986

/6/ ISO 7498/4 OSI Management Framework

/7/ ISO 7498/2 OSI Security Architecture

/8/ Computer Security: The practical issues in a troubled world
Proceedings of the third IFIP International Conference on Computer Security 1986

/9/ Network Security
IEEE Network Magazine, April 1987
Vol. 1, No.2, ss 24-33

/10/ Karila Arto
Tietojärjestelmien suojauspalvelut
Salaus- ja suojausmenetelmät
INSKO, Helsinki 1987

/11/ Ekberg Jan
Tietosuojan kohteet avoimessa järjestelmässä
Salaus- ja suojausmenetelmät
INSKO, Helsinki 1987

/12/ CCITT suositus X.140 1988
Table A-1/X.140

/13/ CCITT suositus X.131 1988
Table 1/X.131

/14/ CCITT suositus X.130 1988
Table 1/X.130
User rate 9600
Statistic 95%
Connection type 1

/15/ CCITT suositus X.130 1988
Table 1/X.131
National portion

/16/ Annex to Question 29/VII
November 1984
Appendix 1 s 2

/17/ CCITT suositus X.130 1988
Table 5/X.130
User rate 9600
Statistic 95%
Connection type 1